



HARMONISED EUROPEAN STANDARD

Cybersecurity (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for firewalls, intrusion detection and/or prevention systems

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please visit: [STAN4CRA / EN 304 636 Firewalls intrusion detection and prevention systems · GitLab](#) and submit your comments as “issues” following the guidelines provided on this site. Alternatively, you may also send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](#)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.



1
2
3
4

Reference

DEN/CYBER-EUS-0020

Keywords

CRA; Cybersecurity; firewall

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

5	Contents		
6	Intellectual Property Rights		7
7	Foreword.....		8
8	Modal verbs terminology		9
9	Introduction		10
10	1 Scope		11
11	2 References		12
12	2.1 Normative references.....		12
13	2.2 Informative references		12
14	3 Definition of terms, symbols and abbreviations.....		13
15	3.1 Terms.....		13
16	3.2 Symbols		14
17	3.3 Abbreviations.....		14
18	4 Product context.....		15
19	4.1 Introduction.....		15
20	4.2 Product functions		15
21	4.2.1 [FN-TI-01] Traffic inspection and analysis.....		15
22	4.2.2 [FN-TD-01] Threat detection and pattern matching.....		15
23	4.2.3 [FN-SP-01] Traffic access control and decision making.....		15
24	4.2.4 [FN-SM-01] Signature and intelligence management.....		15
25	4.3 Product architecture		15
26	4.3.1 General.....		15
27	4.3.2 Product assets		16
28	4.3.3 Product capabilities		16
29	4.4 Operational environment		16
30	4.4.1 General description		16
31	4.4.2 Physical environment.....		16
32	4.4.3 Logical environment		16
33	4.4.4 Connectivity aspects.....		17
34	4.5 Distribution of security functions		17
35	4.6 Users		17
36	4.7 Use cases.....		17
37	4.7.1 General		17
38	4.7.2 Perimeter security deployments		18
39	4.7.3 Internal segmentation deployments.....		18
40	4.7.4 Data centre security deployments.....		18
41	4.7.5 Cloud security deployments		18
42	4.7.6 Distributed branch office protection.....		18
43	4.7.7 Network forensics deployments		18
44	4.7.8 Threat hunting deployments.....		18
45	4.7.9 Host-based security deployments.....		18
46	4.7.10 Application security deployments.....		19
47	4.7.11 Managed security service deployments.....		19
48	5 Technical requirements for the products		20
49	5.1 Introduction.....		20
50	5.2 No known exploitable vulnerabilities		20
51	5.2.1 [KEV-1] No known exploitable vulnerabilities		20
52	5.2.1.1 General		20
53	5.2.1.2 Requirements		20
54	5.3 Secure by default configuration		20
55	5.3.1 [DEFAULT-1] Secure by default configuration		20
56	5.3.1.1 General		20
57	5.3.1.2 Requirements.....		20
58	5.3.2 [RESET-1] Factory reset.....		21
59	5.3.2.1 General		21

60	5.3.2.2	Requirements	21
61	5.4	Secure updates	21
62	5.4.1	[UPDATE-1] Update mechanisms	21
63	5.4.1.1	General	21
64	5.4.1.2	Requirements	21
65	5.5	Authentication and access control	22
66	5.5.1	[AUTH-1] Authentication	22
67	5.5.1.1	General	22
68	5.5.1.2	Requirements	22
69	5.5.2	[AUTH-2] Authorization	23
70	5.5.2.1	General	23
71	5.5.2.2	Requirements	23
72	5.5.3	[AUTH-3] Authenticated session lifecycle	23
73	5.5.3.1	General	23
74	5.5.3.2	Requirements	23
75	5.5.4	[AUTH-4] Protocol access control	23
76	5.5.4.1	General	23
77	5.5.4.2	Requirements	24
78	5.6	Data protection	24
79	5.6.1	General	24
80	5.6.2	Requirements	24
81	5.7	Availability protection	25
82	5.7.1	General	25
83	5.7.2	Requirements	25
84	5.8	Impact minimisation	25
85	5.8.1	General	25
86	5.8.2	Requirements	25
87	5.9	Attack surface and mitigation	25
88	5.9.1	[INTEGRITY-1] System integrity and boot process	25
89	5.9.1.1	General	25
90	5.9.1.2	Requirements	25
91	5.9.2	[PACKET-1] Default packet disposition	26
92	5.9.2.1	General	26
93	5.9.2.2	Requirements	26
94	5.9.3	[EXPOSURE-1] Interface and service exposure minimization	26
95	5.9.3.1	General	26
96	5.9.3.2	Requirements	26
97	5.10	Monitoring and logging	26
98	5.10.1	General	26
99	5.10.2	Requirements	27
100	5.11	Data management	27
101	5.11.1	[TRANSFER-1] Secure data export and transfer	27
102	5.11.1.1	General	27
103	5.11.1.2	Requirements	27
104	5.11.2	[SIGNATURE-1] Signature update and validation	27
105	5.11.2.1	General	27
106	5.11.2.2	Requirements	27
107	5.12	Remote data processing solutions	28
108	5.12.1	General	28
109	5.12.2	Requirements	28
110	6	Assessment criteria for compliance with technical requirements	29
111	6.1	Introduction	29
112	6.2	No known exploitable vulnerabilities	29
113	6.2.1	[KEV-1] No known exploitable vulnerabilities	29
114	6.2.1.1	Requirement assessments	29
115	6.3	Secure by default configuration	31
116	6.3.1	[DEFAULT-1] Secure by default configuration	31
117	6.3.1.1	Requirement assessments	31
118	6.3.2	[RESET-1] Factory reset	41
119	6.3.2.1	Requirement assessments	41
120	6.4	Secure updates	43

121	6.4.1	[UPDATE-1] Update mechanisms	43
122	6.4.1.1	Requirement assessments	43
123	6.5	Authentication and access control	48
124	6.5.1	[AUTH-1] Authentication	48
125	6.5.1.1	Requirement assessments	48
126	6.5.2	[AUTH-2] Authorization	54
127	6.5.2.1	Requirement assessments	54
128	6.5.3	[AUTH-3] Authenticated session lifecycle	57
129	6.5.3.1	Requirement assessments	57
130	6.5.4	[AUTH-4] Protocol access control	62
131	6.5.4.1	Requirement assessments	62
132	6.6	Data protection	66
133	6.6.1	Requirement assessments	66
134	6.7	Availability protection	69
135	6.7.1	Requirement assessments	69
136	6.8	Impact minimisation	72
137	6.8.1	Requirement assessments	72
138	6.9	Attack surface and mitigation	73
139	6.9.1	[INTEGRITY-1] System integrity and boot process	73
140	6.9.1.1	Requirement assessments	73
141	6.9.2	[PACKET-1] Default packet disposition	77
142	6.9.2.1	Requirement assessments	77
143	6.9.3	[EXPOSURE-1] Interface and service exposure minimization	81
144	6.9.3.1	Requirement assessments	81
145	6.10	Monitoring and logging	83
146	6.10.1	Requirement assessments	83
147	6.11	Data management	86
148	6.11.1	[TRANSFER-1] Secure data export and transfer	86
149	6.11.1.1	Requirement assessments	86
150	6.11.2	[SIGNATURE-1] Signature update and validation	89
151	6.11.2.1	Requirement assessments	89
152	6.12	Remote data processing solutions	95
153	6.12.1	Requirement assessments	95
154	Annex A (informative): Relationship between the present document and the requirements of		
155	EU Regulation (EU) 2024/2847 — the Cyber Resilience Act		99
156	Annex B (informative): Security analysis		102
157	B.1	General	102
158	B.2	Threat landscape	102
159	B.2.1	Threats related to vulnerability handling	102
160	B.2.2	Threats related to access control and authentication	102
161	B.2.3	Threats related to availability and inspection bypass	103
162	B.2.4	Threats related to integrity and tampering	103
163	B.2.5	Threats related to signature and intelligence integrity	104
164	B.2.6	Threats related to data protection	104
165	B.2.7	Threats related to monitoring and visibility	104
166	B.2.8	Threats related to default configuration	104
167	B.2.9	Threats related to physical and deployment security	105
168	B.2.10	Threats related to detection disruption	105
169	B.3	Threat assessment framework	105
170	B.3.1	Introduction	105
171	B.3.2	Risk factors	106
172	B.3.2.1	Baseline risk factors	106
173	B.3.2.2	Traffic inspection risk factors	106
174	B.3.2.3	Update and intelligence risk factors	107
175	B.3.2.4	Deployment architecture risk factors	107
176	B.3.2.5	Data operations risk factors	107
177	B.3.2.6	Remote data processing risk factors	107
178	B.3.3	Threat justification and mitigation	108
179			
180			

182 Intellectual Property Rights

183 Essential patents

184 IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations
185 pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be
186 found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to*
187 *ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the
188 [ETSI IPR online database](#).

189 Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs,
190 including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not
191 referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become,
192 essential to the present document.

193 Trademarks

194 The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners.
195 ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no
196 right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does
197 not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

198 **DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its
199 Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the
200 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of
201 the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

202

203

Foreword

204 This draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cybersecurity (TC
205 CYBER) and is now submitted for the combined Public Enquiry and Vote phase of the ETSI EN Approval Procedure.

206 The present document has been prepared under the Commission's standardisation request C(2025)618 [i.3] to provide
207 one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 [i.1] of the European Parliament
208 and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and
209 amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, known as the Cyber
210 Resilience Act (CRA).

211 Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance
212 with the normative clauses of the present document given in table A.1 confers, within the limits of the scope of the
213 present document, a presumption of conformity with the corresponding requirements of that Regulation and associated
214 EFTA regulations.

Proposed national transposition dates

Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

215

216 Modal verbs terminology

217 In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and
218 "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of
219 provisions).

220 "**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

221

222

Introduction

223

The present document covers cybersecurity for firewalls, intrusion detection systems, and intrusion prevention systems.

224

These products are identified in Annex III, Class II, point 2 of Regulation (EU) 2024/2847 [\[i.1\]](#), known as the Cyber

225

Resilience Act (CRA).

226

The present document provides a structured approach to identify the applicable cybersecurity requirements for the

227

products in scope, following a risk-based approach. Security controls are therefore proportionate to the intended

228

purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

229

Clause [4](#) describes the product architecture and intended purpose, and defines the use cases for the main deployment

230

scenarios under reasonably foreseeable use.

231

Clause [5](#) specifies the technical cybersecurity requirements for the product to mitigate the identified risks.

232

Clause [6](#) specifies the assessment criteria and compliance verification procedures for the requirements of clause [5](#).

233

Annex [A](#) maps the technical requirements of the present document to the corresponding cybersecurity requirements of

234

the CRA [\[i.1\]](#).

235

Annex [B](#) describes the methodology used to assess the security risks of the products in their context. Where a product

236

does not clearly correspond to one of the use cases defined in clause [4](#), the risk assessment methodology of Annex [B](#)

237

may be used to determine the applicable cybersecurity requirements.

238

239

1 Scope

240

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for firewalls, intrusion detection systems, and intrusion prevention systems related to cybersecurity. The products with digital elements in scope:

241

242

243

- are specified within the "technical description" of the "category of product" in Class II, point 2 by the Commission Implementing Regulation 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council [\[i.1\]](#) as:

244

245

246

247

- "Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network.

248

249

250

This category includes but is not limited to network firewalls and application firewalls such as web application firewalls or filters and anti-spam gateways.";

251

252

- "Intrusion detection systems are products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system.

253

254

255

This category includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.";

256

257

- "Intrusion prevention systems are products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system.

258

259

This category includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.";

260

261

- are only covered within the product context described in clause [4](#).

262

The present document addresses the cybersecurity requirements of CRA [\[i.1\]](#), Annex I, Part I and Part II.

263

Firewalls, intrusion detection systems, and intrusion prevention systems fall within the scope of the present document, whether deployed as physical appliances or software. The present document applies when the intended purpose or reasonably foreseeable use involves monitoring, analysing, or controlling network traffic for security purposes.

264

265

266

Products that detect access attempts made without authorization, identify malicious activity, or enforce traffic controls to protect networks and systems from intrusions are within scope.

267

268

The present document does not specify how products detect threats, classify traffic, or implement inspection algorithms.

269

Detection accuracy rates, false positive thresholds, and signature effectiveness metrics are outside scope. Security requirements for the robustness of protocol parsing engines, the integrity of inspection processes, and vulnerability management remain within scope.

270

271

272

273 2 References

274 2.1 Normative references

275 References are either specific (identified by date of publication and/or edition number or version number) or non-
276 specific. For specific references, only the cited version applies. For non-specific references, the latest version of the
277 referenced document (including any amendments) applies.

278 Referenced documents which are not found to be publicly available in the expected location might be found in the
279 ETSI docbox.

280 NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee
281 their long-term validity.

282 The following referenced documents are necessary for the application of the present document.

283 [1] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary",
284 (produced by CEN/CENELEC).

285 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

286 [2] prEN 40000-1-2: "Cybersecurity requirements for products with digital elements - Part 1-2:
287 Principles for cyber resilience", (produced by CEN/CENELEC).

288 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

289 [3] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Part 1-3:
290 Vulnerability Handling", (produced by CEN/CENELEC).

291 NOTE: Version and date to be added upon its publication by CEN/CENELEC.

292 2.2 Informative references

293 References are either specific (identified by date of publication and/or edition number or version number) or non-
294 specific. For specific references, only the cited version applies. For non-specific references, the latest version of the
295 referenced document (including any amendments) applies.

296 NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee
297 their long-term validity.

298 The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's
299 understanding but are not required for conformance to the present document.

300 [i.1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on
301 horizontal cybersecurity requirements for products with digital elements and amending
302 Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber
303 Resilience Act).

304 [i.2] Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical
305 description of the categories of important and critical products with digital elements pursuant to
306 Regulation (EU) 2024/2847 of the European Parliament and of the Council.

307 [i.3] Standardisation request M/606 - C(2025)618: "Commission Implementing decision of 3.2.2025 on
308 a standardisation request to the European Committee for Standardisation (CEN), the European
309 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
310 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
311 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
312 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
313 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".

314 [i.4] NIST SP 800-133 Rev. 2 (June 2020): "Recommendation for Cryptographic Key Generation".

315

316 3 Definition of terms, symbols and abbreviations

317 3.1 Terms

318 For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], prEN 40000-1-1 [1] and
319 the following apply:

320 **audit event:** timestamped, structured record of activities including authentication attempts, configuration changes,
321 system events, and administrative actions

322 **critical security parameter:** confidential information whose disclosure or modification can compromise product
323 security

324 **cryptographic algorithm:** sequence of instructions based on mathematical properties to protect confidentiality,
325 integrity or authenticity against attacks

326 **diagnostic interface:** interface used for diagnostic or troubleshooting purposes, not part of the intended function of the
327 product

328 **factory reset:** mechanism that restores the product to product factory default state

329 **fail-open operation:** operation of the product in which traffic that cannot be inspected is forwarded without applying a
330 fail-secure action

331 NOTE: Fail-open operation may result from software configuration, hardware bypass, inspection or signature
332 update windows, or per-flow bypass configuration.

333 **fail-secure action:** configured action applied by the product to traffic that cannot be inspected, such that the traffic is
334 not forwarded without inspection

335 NOTE: Typical fail-secure actions include drop, block, reject, and quarantine.

336 **firewalls:** products with digital elements that protect a connected network or system from access made without
337 authorization by monitoring and restricting data communication traffic to and from that network or between nodes of
338 that network

339 NOTE: This includes but is not limited to network firewalls and application firewalls such as web application
340 firewalls (WAF), anti-spam gateways and content filtering systems.

341 **firmware:** software stored in non-volatile memory that controls product operation

342 NOTE 1: Firmware includes boot sequences, operating system components, inspection engines, and management
343 interfaces.

344 NOTE 2: Firmware may include persistent configuration data required for product operation.

345 **intrusion detection systems:** products with digital elements that monitor traffic once it has entered the network
346 environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has
347 occurred on a connected network or system

348 NOTE: This includes but is not limited to network-based intrusion detection systems and host-based intrusion
349 detection systems.

350 **intrusion prevention systems:** products with digital elements composed of an intrusion detection system that actively
351 responds to an intrusion to a connected network or system

352 NOTE: This includes but is not limited to network-based intrusion prevention systems and host-based intrusion
353 prevention systems.

354 **management override:** deliberate configuration action by a privileged management account that (i) enables a non-
355 default product behavior; and (ii) is distinguishable from routine product configuration

356 NOTE: Mechanisms that satisfy management override include confirmation prompts acknowledging the
357 consequence of the override, reauthentication for the override action, and separate management
358 workflows for non-default behaviors. Default configuration values and settings inherited from templates
359 are not management overrides.

- 360 **network interface:** physical interface that can be used to access the functionality of firewall, IDS or IPS via a network
- 361 **product:** firewall, intrusion detection system, or intrusion prevention system within the scope of the present document
- 362 **product factory default state:** state of the product as configured by the manufacturer before initial setup, to which it
363 returns after a factory reset
- 364 **product operational state:** state of the product after initial setup is complete, with no further configuration changes
- 365 **remote data processing solution:** data processing at a distance for which the software is designed and developed by
366 the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product
367 from performing one of its functions
- 368 NOTE: SOURCE: Regulation (EU) 2024/2847, Article 3, point 2 [\[i.1\]](#).
- 369 **secure channel:** path for transferring data between two entities or components that ensures confidentiality, integrity,
370 and replay protection, as well as mutual authentication between the entities or components
- 371 NOTE 1: The secure channel may be provided using cryptographic, physical, or procedural methods or a
372 combination thereof.
- 373 NOTE 2: SOURCE: NIST SP 800-133 Rev. 2 [\[i.4\]](#).
- 374 **secure-by-default configuration:** configuration in which the product satisfies requirements in clause [5.3.1](#)
- 375 **security rule:** specific statement or entry that specifies source, destination, protocol, port, action, and matching criteria
376 for traffic classification
- 377 NOTE: Multiple rules may collectively express a single set of security decisions.
- 378 **signature database:** collection of patterns, heuristics, and indicators used by the product to detect known threats during
379 traffic inspection
- 380 **software bill of materials:** formally structured list of all software components, libraries, and dependencies included in
381 the product, with version identifiers

382 3.2 Symbols

383 Void.

384 3.3 Abbreviations

385 For the purposes of the present document, the following abbreviations apply:

API	Application Programming Interface
CRA	Cyber Resilience Act
DoS	Denial of Service
EU	European Union
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
JTAG	Joint Test Action Group
RDPS	Remote Data Processing Solution
SIEM	Security Information and Event Management
SBOM	Software Bill of Materials
SOC	Security Operations Centre
SWD	Serial Wire Debug
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver-Transmitter
WAF	Web Application Firewall

386

387 4 Product context

388 4.1 Introduction

389 Firewalls, intrusion detection systems, and intrusion prevention systems protect network boundaries by inspecting
390 traffic and enforcing configured rules. Their position at network boundaries protects integrity, confidentiality, and
391 availability.

392 Compromise of these products can affect the security of all networks and systems that depend on them for protection.
393 Security measures scale with deployment context whilst maintaining baseline protections.

394 Firewalls filter traffic using rules and stateful inspection. Intrusion detection systems monitor traffic and generate alerts.
395 Intrusion prevention systems actively block threats. All three analyse traffic, maintain state information, balance
396 detection accuracy against false positives, and protect themselves whilst performing security functions. Products can be
397 deployed as dedicated appliances, built into the network infrastructure, obtained as a managed service, or installed on
398 individual hosts. Security measures protect both the inspection function and management interfaces based on product
399 capabilities and deployment.

400 Manufacturers add functionality such as threat intelligence, machine learning analytics, and cloud management. Each
401 adds attack surfaces that require security assessment and maintenance.

402 4.2 Product functions

403 4.2.1 [\[FN-TI-01\]](#) Traffic inspection and analysis

404 This function parses and examines network traffic across protocol layers. Inspection covers packet headers, stateful
405 protocol tracking, application identification, and content analysis. Engines handle fragment reassembly, protocol
406 decoding, and state tracking. Firewalls, intrusion detection systems, and intrusion prevention systems all use this
407 function as the basis for detection and enforcement decisions.

408 4.2.2 [\[FN-TD-01\]](#) Threat detection and pattern matching

409 This function identifies known and unknown threats using inspected traffic. Signature-based detection matches traffic
410 against known attack patterns, malware, and exploits. Anomaly detection builds behaviour baselines and flags
411 deviations that indicate compromise. Behavioural analysis tracks entities over time to detect subtle threat indicators that
412 individual events miss. Intrusion detection systems generate alerts based on detection results. Intrusion prevention
413 systems use detection results to block or mitigate threats in real time.

414 4.2.3 [\[FN-SP-01\]](#) Traffic access control and decision making

415 This function evaluates traffic against configured rules to permit, block, log, or modify communications. Firewalls
416 implement rules based on source, destination, service, time, user identity, and application context. Intrusion prevention
417 systems add automatic threat blocking, traffic quarantine, and rate limiting. Intrusion detection systems do not enforce
418 rules but may generate alerts that inform enforcement decisions on other products. The rule engine evaluates entries in
419 priority order, handles conflicts consistently, and applies default actions to unmatched traffic.

420 4.2.4 [\[FN-SM-01\]](#) Signature and intelligence management

421 This function maintains signature and rule databases used by the detection function. Management retrieves updates,
422 validates integrity and compatibility, and stages signatures for testing. It manages custom and vendor rules and
423 optimizes for performance. This function applies to intrusion detection and intrusion prevention systems that use
424 signature-based detection, and to firewalls that use application-layer inspection signatures. Threat intelligence feeds
425 enable dynamic updates from emerging threats and local observations.

426 4.3 Product architecture

427 4.3.1 General

428 Products inspect traffic and enforce configured rules across one or more protocol layers. Network firewalls and
429 intrusion prevention systems operate inline, processing traffic between network segments. Application firewalls operate

430 at the application layer, inspecting protocol-specific content. Products may use dedicated hardware, custom engines,
431 and distributed designs.

432 The software architecture builds on specialized operating systems optimized for security processing and real-time traffic
433 analysis. Security engines implement signature-based pattern matching, behavioural analysis, and threat detection
434 algorithms. Management software provides configuration tools, rule management, and logging. It integrates with SIEM
435 platforms. Security controls span management access, encrypted channels, and inline inspection.

436 Manufacturers add further capabilities such as threat intelligence, cloud management, and security orchestration. Each
437 adds attack surfaces that require security assessment and maintenance.

438 4.3.2 Product assets

439 [\[AS-FW-01\]](#) Security policies and rule sets

440 [\[AS-FW-02\]](#) Signature databases and threat intelligence

441 [\[AS-FW-03\]](#) Inspection engine state

442 [\[AS-FW-04\]](#) Audit event records

443 4.3.3 Product capabilities

444 [\[CAP-FW-01\]](#) Deep packet inspection

445 [\[CAP-FW-02\]](#) Stateful traffic analysis

446 [\[CAP-FW-03\]](#) Signature-based threat detection

447 [\[CAP-FW-04\]](#) Inline traffic enforcement

448 4.4 Operational environment

449 4.4.1 General description

450 Products covered by the present document operate in diverse environments. Environments differ by product type as
451 described in clause [4.1](#), by the deployment form, and by the operational context. Deployment forms include physical
452 appliances, virtual machines, and containers. Relevant factors are network architecture, trust boundaries, traffic
453 volumes, tolerance for downtime, and the level of integration with security ecosystems.

454 Products operate at network enforcement points processing traffic between networks with different trust levels. They
455 inspect traffic that may be malicious while themselves being targets of attack.

456 4.4.2 Physical environment

457 Physical environments range from data centres with strict access controls and dedicated equipment rooms to branch
458 offices and retail locations. Physical appliances may be rack-mounted in secured facilities or deployed as desktop units
459 in office environments. Physical protection varies from controlled-access server rooms to open office spaces where the
460 product may be accessible to non-technical personnel.

461 4.4.3 Logical environment

462 Products are deployed at network boundaries, between internal segments, or as host-based agents. In perimeter
463 deployments, the product is the primary security boundary between the internal network and the public network. In
464 segmentation deployments, products enforce trust boundaries between internal zones. Virtual and cloud deployments
465 may share compute resources with protected workloads.

466 Management access is provided through dedicated management interfaces, in-band management over the data network,
467 or cloud-based management platforms. The choice of management architecture affects the attack surface and the
468 distribution of security functions.

469 4.4.4 Connectivity aspects

470 Products connect to multiple network segments simultaneously. Perimeter products connect to at least one untrusted
471 external network and one or more internal networks. Segmentation products connect to two or more internal network
472 segments. Host-based products connect to the host operating system network stack.

473 Integration with security ecosystems can include SIEM platforms, threat intelligence feeds, orchestration systems, and
474 incident response tools. These integrations require network connectivity to external services and introduce additional
475 interfaces that the product exposes.

476 4.5 Distribution of security functions

477 Security functions of the product are distributed across the product architecture described in 4.3. Where the product
478 relies on remote data processing solutions for cloud management, threat intelligence, signature distribution, or log
479 collection, the distribution extends to the RDPS boundary as described in clause 5.12. The risk factors defined in B.3
480 determine which security requirements from clause 5 apply to a specific product based on its intended purpose,
481 reasonably foreseeable use, and conditions of use.

482 4.6 Users

483 Firewalls, intrusion detection systems, and intrusion prevention systems may be accessed by multiple categories of
484 users each having different roles, needs and privileges.

485 Security administrators configure access control rules, update signatures, and modify system settings determining
486 permitted or blocked traffic. They have deep knowledge of security architectures, threat landscapes, and risk tolerance.
487 This role requires strong authentication and comprehensive audit logging. Significant configuration changes may be
488 subject to multiple approvals from security and network teams.

489 Security analysts and incident responders monitor alerts continuously, investigate threats, and tune detection rules to
490 reduce false positives. They require read access to security events, packet captures, and threat intelligence, plus limited
491 write access for suppression rules and alert acknowledgement. This role requires strong authentication and
492 comprehensive audit logging.

493 Network administrators require limited access for troubleshooting connectivity issues or coordinating changes affecting
494 traffic flows. Whilst not primarily responsible for security functions, they need visibility into rules blocking legitimate
495 traffic and ability to request modifications through documented channels. Access is restricted to viewing relevant rules
496 and logs without modifying security controls.

497 Compliance auditors and security assessors require read-only access to verify correct configuration and effective
498 operation. They review rules, examine audit logs, and generate compliance reports without modifying configurations.
499 Access can be temporary, restricted to compliance functions, with all activities logged.

500 Automated systems and orchestration platforms interact through APIs requiring service accounts with scoped
501 permissions. They update threat intelligence, deploy configuration changes, collect logs, or implement response actions.
502 Access requires strong authentication using certificates or API keys, with permissions limited to necessary functions.
503 Compromise of automated accounts could disable security controls across multiple products simultaneously.

504 SOC personnel work in staffed environments and monitor multiple products through centralized consoles. They require
505 streamlined interfaces for rapid threat identification and response across multiple customer environments. Access
506 patterns involve shift handovers, escalation procedures, and coordinated incident response. SOC operators have read-
507 only access with limited ability to implement temporary countermeasures under change control.

508 Security product users understand threat landscapes, attack techniques, and defensive strategies. Products cannot rely on
509 intuitive interfaces alone but provide detailed information about threats, rule logic, and detection confidence for
510 informed decisions. Misconfigurations cause security breaches, not just service disruptions. User training and clear
511 documentation are essential.

512 4.7 Use cases

513 4.7.1 General

514 This clause identifies use cases for firewalls, intrusion detection systems, and intrusion prevention systems. The use
515 cases presented are neither exhaustive nor mutually exclusive. A single product can support multiple use cases. The list
516 of use cases can be extended in future revisions of the present document.

517 The description of each use case is limited to those characteristics considered relevant for the identification of threats.
518 Characteristics may be both the user categories and their properties as described in clause [4.6](#) as well as the operational
519 environments and their properties as described in clause [4.4](#).

520 4.7.2 Perimeter security deployments

521 This use case covers deployments where firewalls establish the primary security boundary between internal networks
522 and untrusted external networks. External networks in this context include the public internet. The firewall is positioned
523 as the sole traffic path, blocking all traffic except explicitly permitted communications. Products inspect both inbound
524 and outbound traffic. Inbound inspection protects internal resources; outbound inspection identifies data exfiltration or
525 malware communication. Deployments face continuous automated attacks and reconnaissance, requiring robust
526 logging, alerting, and automated response. Mission-critical perimeter deployments may use redundant product clusters
527 with state synchronization and automatic failover.

528 4.7.3 Internal segmentation deployments

529 This use case covers deployments where firewalls and intrusion prevention systems are deployed between internal
530 network segments to enforce zero-trust rules and limit lateral movement after compromise. Internal boundaries separate
531 departments, isolate critical systems, and create demilitarized zones for public services. Products handle high east-west
532 traffic volumes at low latency. They detect abnormal behaviour, access attempts between segments made without
533 authorization, and lateral movement.

534 4.7.4 Data centre security deployments

535 This use case covers deployments where products protect virtualized workloads within data centre environments.
536 Products operate as virtual appliances or are integrated into the virtualization infrastructure. Deployments protect
537 workloads that migrate between hosts and share compute resources. Products enforce segmentation between tenant
538 environments and between production, development, and management zones.

539 4.7.5 Cloud security deployments

540 This use case covers deployments where security inspection is distributed through cloud-native controls and container-
541 native firewalls. Products integrate with orchestration platforms and SDN controllers. Workloads scale dynamically and
542 exist temporarily. Rules follow workloads across cloud infrastructure. Where these deployments rely on remote data
543 processing solutions, clause [5.12](#) applies.

544 4.7.6 Distributed branch office protection

545 This use case covers deployments at branch offices providing local inspection without backhauling traffic to centralized
546 data centres. Deployments range from small, unified threat management appliances protecting few users to regional
547 hubs aggregating traffic from multiple locations. Branch deployments run with minimal local IT support. They require
548 simple management interfaces, automated threat response, and centralized configuration management.

549 4.7.7 Network forensics deployments

550 This use case covers deployments of dedicated intrusion detection systems for post-incident forensic analysis. Sensors
551 capture and record network traffic for evidence preservation and historical investigation. Deployments emphasize
552 comprehensive packet capture, metadata generation, and long-term storage. Products operate in passive mode observing
553 all traffic without blocking.

554 4.7.8 Threat hunting deployments

555 This use case covers deployments where intrusion detection systems support proactive searching for threats that evade
556 automated detection. Analysts use the product to test hypotheses about attacker presence by querying traffic patterns,
557 correlating events, and identifying anomalies. Products provide visibility into network activity and support integration
558 with threat intelligence for indicator matching.

559 4.7.9 Host-based security deployments

560 This use case covers products installed on individual servers, workstations, or endpoints rather than as dedicated
561 network appliances. Host-based products inspect traffic at the operating system level. They enforce rules based on the
562 local application context. They protect individual systems against threats that bypass network-level inspection, such as
563 lateral movement within a trusted segment.

564 4.7.10 Application security deployments

565 This use case covers products that inspect traffic at the application layer. Web application firewalls protect web services
566 by inspecting HTTP and HTTPS traffic for injection attacks, cross-site scripting, and protocol violations. Anti-spam
567 gateways and content filtering systems inspect email and web traffic for unwanted or malicious content. These products
568 operate as reverse proxies or inline filters and require application-layer protocol awareness beyond network packet
569 inspection.

570 4.7.11 Managed security service deployments

571 This use case covers managed security service providers that protect multiple customer networks through shared or
572 dedicated products. Customer traffic is isolated. Products support virtual domains, separate routing tables, and isolated
573 rule sets. Information does not leak between customers. Where these deployments rely on remote data processing
574 solutions, clause [5.12](#) applies.

575

576 5 Technical requirements for the products

577 5.1 Introduction

578 The technical requirements of the present document apply under the product context described in clause 4, which shall
579 be in accordance with its intended use. The equipment shall comply with all applicable technical requirements of the
580 present document at all times when operating in such product context.

581 Conditional applicability ensures measures are proportionate to the risks arising from the intended purpose, reasonably
582 foreseeable use, deployment context, and threat exposure.

583 5.2 No known exploitable vulnerabilities

584 5.2.1 [KEV-1] No known exploitable vulnerabilities

585 5.2.1.1 General

586 The product shall be made available on the market without known exploitable vulnerabilities. The manufacturer shall
587 maintain a software bill of materials covering all product components and third-party dependencies. The assessor
588 verifies the software bill of materials against known vulnerability databases.

589 5.2.1.2 Requirements

590 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (a).

591 [\[RO-KEV-1-01\]](#) The manufacturer shall maintain a software bill of materials for each product version in a machine-
592 readable format.

593 [\[RO-KEV-1-02\]](#) The product shall contain no known exploitable vulnerabilities in each product version when made
594 available on the market.

595 [\[RO-KEV-1-03\]](#) The manufacturer shall verify that third-party components in the product do not contain known
596 exploitable vulnerabilities before making each product version available on the market.

597 5.3 Secure by default configuration

598 5.3.1 [DEFAULT-1] Secure by default configuration

599 5.3.1.1 General

600 Products shall include security controls that are configured and enabled from initial deployment. This protects against
601 exploitation attempts that can occur within minutes of network connection. The default configuration establishes the
602 security baseline that many deployments operate with unchanged throughout the product lifecycle.

603 5.3.1.2 Requirements

604 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (b).

605 [\[RO-DEFAULT-1-01\]](#) The product, in its product factory default state, shall enforce the applicable requirements of the
606 present document. The product need not enforce a requirement when (i) that requirement renders the initial product
607 setup process non-functional; and (ii) the instructions to the user document the exception.

608 [\[RO-DEFAULT-1-02\]](#) The product, in its product factory default state, shall enable only those interfaces and services
609 that product setup requires.

610 [\[RO-DEFAULT-1-03\]](#) The product, in its product operational state, shall enforce all applicable requirements of the
611 present document.

612 [\[RO-DEFAULT-1-04\]](#) The product, in its product factory default state, shall restrict access to accounts and methods
613 documented in the instructions to the user.

614 [\[RO-DEFAULT-1-05\]](#) The product, in its product operational state, shall restrict access to accounts and authentication
615 methods explicitly configured by the user.

616 [\[RQ-DEFAULT-1-06\]](#) For credentials that are documented in the instructions to the user, the product, in its product
617 factory default state, shall enforce change of those credentials.

618 [\[RQ-DEFAULT-1-07\]](#) The product shall (i) disable all diagnostic interfaces by default; and (ii) where the product
619 provides configuration to enable a diagnostic interface, protect that interface with authentication and authorization.

620 [\[RQ-DEFAULT-1-08\]](#) The product shall generate audit events for product errors.

621 [\[RQ-DEFAULT-1-09\]](#) The product shall require state of the art cryptography for all cryptographic functions.

622 NOTE: This requirement is subject to review once Annex K is available.

623 [\[RQ-DEFAULT-1-10\]](#) The product shall not support protocols with known exploitable vulnerabilities.

624 [\[RQ-DEFAULT-1-11\]](#) The product shall enable mitigations for known design limitations of protocols terminated by the
625 product.

626 [\[RQ-DEFAULT-1-12\]](#) The product shall enforce the principle of least privilege during normal operation.

627 [\[RQ-DEFAULT-1-13\]](#) The product shall store audit events in persistent memory that survives a reboot.

628 5.3.2 [RESET-1] Factory reset

629 5.3.2.1 General

630 Factory reset mechanisms remove all data and user configurations while leaving the current running software and the
631 firmware versions in place. The factory reset also deletes the user login credentials, leading to the initial setup
632 procedures.

633 NOTE 1: Factory reset does not include other types of reset procedures, such as what is commonly known as
634 "operational reset" or "operator reset", where user data and configuration are preserved.

635 NOTE 2: In virtual environments, an alternative to factory reset of an existing instance may be to launch a new
636 instance with the default configuration.

637 5.3.2.2 Requirements

638 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (b).

639 [\[RQ-RESET-1-01\]](#) The product shall provide a factory reset mechanism that restores the product to its secure-by-
640 default configuration.

641 NOTE: The product may provide a physical factory reset mechanism that does not require authentication.

642 [\[RQ-RESET-1-02\]](#) The product shall provide a factory reset mechanism that maintains the currently installed firmware
643 version and all installed security updates.

644 [\[RQ-RESET-1-03\]](#) The product shall not retain (i) previous configuration; (ii) user data; or (iii) critical security
645 parameters after factory reset.

646 5.4 Secure updates

647 5.4.1 [UPDATE-1] Update mechanisms

648 5.4.1.1 General

649 This clause establishes requirements for delivering and installing security updates to address vulnerabilities throughout
650 the product lifetime. Products may remain deployed for extended periods and may serve as critical infrastructure.
651 Robust update mechanisms maintain security against evolving threats.

652 5.4.1.2 Requirements

653 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (c).

654 [\[RQ-UPDATE-1-01\]](#) The product shall provide a mechanism to receive security updates.

655 [\[RQ-UPDATE-1-02\]](#) The product shall prevent installation of security updates without authentication and without
656 authorization.

657 [\[RQ-UPDATE-1-03\]](#) The product shall install a received security update and report the installed version.

658 [\[RQ-UPDATE-1-04\]](#) The product shall retry failed security update delivery and installation attempts.

659 [\[RQ-UPDATE-1-05\]](#) Where the product supports on-product delivery, the product shall enable by default an automated
660 mechanism that detects available security updates.

661 [\[RQ-UPDATE-1-06\]](#) The product shall verify security update integrity using state of the art cryptography before
662 installation.

663 NOTE: This requirement is subject to review once Annex K is available.

664 [\[RQ-UPDATE-1-07\]](#) The product shall generate audit events for (i) security update availability; (ii) security update
665 download initiation, completion, or failure; and (iii) security update installation success or failure.

666 5.5 Authentication and access control

667 5.5.1 [AUTH-1] Authentication

668 5.5.1.1 General

669 Authentication is the fundamental security barrier against product modification without authorization. These products
670 play a critical role in network security enforcement. Compromise of access controls can disable threat detection, bypass
671 security rules, or grant access to protected networks. This clause establishes requirements to ensure only authorized
672 users can access product management functions.

673 5.5.1.2 Requirements

674 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

675 [\[RQ-AUTH-1-01\]](#) The product shall require user authentication on all interfaces providing access to the product.

676 [\[RQ-AUTH-1-02\]](#) The product shall provide unique credentials per product unit during secure production.

677 [\[RQ-AUTH-1-03\]](#) Where the product transmits critical security parameters, the product shall protect their transmission
678 over a secure channel.

679 NOTE: This requirement is subject to review once Annex K is available.

680 [\[RQ-AUTH-1-04\]](#) The product shall protect critical security parameters using state of the art cryptography.

681 NOTE: This requirement is subject to review once Annex K is available.

682 [\[RQ-AUTH-1-05\]](#) The product shall enforce minimum credential entropy requirements.

683 NOTE: This requirement is subject to review once Annex K is available.

684 [\[RQ-AUTH-1-06\]](#) The product shall enforce authentication failure protection, including (i) progressive delays between
685 failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

686 [\[RQ-AUTH-1-07\]](#) The product shall (i) store previously used passwords using state of the art cryptography; (ii) validate
687 password changes against this history before acceptance; and (iii) store previous passwords to at least the depth that is
688 given in table 1.

689 **Table 1: Minimum password history depth**

Risk scope	Minimum value	Applicable risk factors
Baseline	1	—
Local or internal network management	6	RF-B-06
Internet-exposed management	12	RF-B-06, RF-TI-02

690 5.5.2 [AUTH-2] Authorization

691 5.5.2.1 General

692 This clause establishes requirements for controlling what authenticated users can do on the product. While
693 authentication verifies user identity, access control ensures users can only perform actions permitted by their privilege
694 level. This is critical for the product as different users require different privileges.

695 5.5.2.2 Requirements

696 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

697 [\[RQ-AUTH-2-01\]](#) Where the product supports more than one privilege level, the product shall enforce privilege
698 separation.

699 [\[RQ-AUTH-2-02\]](#) The product shall restrict each user to their authorized privilege level.

700 [\[RQ-AUTH-2-03\]](#) The product shall enforce access control on all interfaces providing access to the product.

701 [\[RQ-AUTH-2-04\]](#) The product shall validate each command based on the authorized privilege level before execution.

702 5.5.3 [AUTH-3] Authenticated session lifecycle

703 5.5.3.1 General

704 This clause establishes requirements for managing the lifecycle of authenticated sessions, from establishment through
705 termination. The product shall maintain the security context created through authentication as specified in clause [5.5.1](#)
706 and authorization as specified in clause [5.5.2](#) throughout the interaction. Session management prevents access without
707 authorization through session compromise.

708 Products remain accessible continuously and may be managed from multiple locations and interfaces. Robust session
709 controls prevent configuration changes without authorization that could compromise entire network segments.
710 Vulnerabilities such as session hijacking, fixation, or replay attacks can lead to full product compromise, even when
711 strong authentication is in place.

712 5.5.3.2 Requirements

713 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

714 [\[RQ-AUTH-3-01\]](#) The product shall generate session identifiers that are unique, non-predictable, and resistant to brute
715 force attacks, using state of the art cryptography.

716 NOTE: This requirement is subject to review once Annex K is available.

717 [\[RQ-AUTH-3-02\]](#) The product shall enforce session timeout with configurable idle timeout periods and default values.

718 [\[RQ-AUTH-3-03\]](#) The product shall invalidate sessions immediately upon (i) session logout or termination; (ii)
719 authentication credential change; or (iii) timeout expiration.

720 [\[RQ-AUTH-3-04\]](#) The product shall restrict session identifiers to the session management mechanism.

721 NOTE: This requirement is subject to review once Annex K is available.

722 [\[RQ-AUTH-3-05\]](#) The product shall limit concurrent sessions to a configurable maximum per user account.

723 [\[RQ-AUTH-3-06\]](#) The product shall deny privilege escalation attempts without authorization within active sessions.

724 5.5.4 [AUTH-4] Protocol access control

725 5.5.4.1 General

726 This clause establishes requirements for administrative control over network protocols available on the product. The
727 product shall permit only authenticated and authorized users to enable, disable, or configure network protocols.
728 Management protocols shall use state of the art cryptography, and the product shall warn when cleartext or weak
729 protocols are enabled.

730 5.5.4.2 Requirements

731 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (d).

732 Where risk factor [RF-B-06] is present, requirement [RQ-AUTH-4-01] applies.

733 [\[RQ-AUTH-4-01\]](#) The product shall enable only management protocols using state of the art cryptography in product
734 factory default state and in product operational state.

735 NOTE: This requirement is subject to review once Annex K is available.

736 Where any of risk factors [RF-B-05], [RF-TI-02] is present, requirement [RQ-AUTH-4-02] applies.

737 [\[RQ-AUTH-4-02\]](#) The product shall enforce rate limiting for each protocol that accepts requests without authentication.

738 Where risk factor [RF-B-06] is present, requirement [RQ-AUTH-4-03] applies.

739 [\[RQ-AUTH-4-03\]](#) The product shall provide capability to configure state of the art cryptography and to disable
740 protocols that do not use state of the art cryptography.

741 [\[RQ-AUTH-4-04\]](#) The product shall (i) validate trust establishment using additional mechanisms; and (ii) generate audit
742 events for all trust relationship changes.

743 5.6 Data protection

744 5.6.1 General

745 This clause establishes requirements for data confidentiality, integrity, and minimization. Confidentiality ensures data is
746 accessible only to authorized entities. Integrity ensures data cannot be modified without authorization. Data
747 minimization limits collection and retention to what the intended functions require.

748 These principles apply to all data types processed by the product. Traffic content accessed during security inspection is
749 subject to the same protections.

750 NOTE 1: Data necessary for intended security inspection functions includes connection state tables, signature
751 matching results, threat detection metadata, security rule evaluation context, and session tracking data. It
752 also includes inspection engine state, rule decision logs, and alert correlation data.

753 NOTE 2: Data considered beyond the intended purpose includes long-term retention of full packet payloads beyond
754 real-time inspection, per-device behavioural analytics such as browsing habits or usage patterns, device
755 fingerprinting beyond what access control requires, and diagnostic or telemetry data sent to the
756 manufacturer or third parties.

757 5.6.2 Requirements

758 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (e), (2) (f) and (2) (g).

759 [\[RQ-DATA-1-01\]](#) The product shall encrypt data at rest using state of the art cryptography.

760 NOTE: This requirement is subject to review once Annex K is available.

761 [\[RQ-DATA-1-02\]](#) The product shall encrypt management communications and control plane traffic using state of the
762 art cryptography.

763 NOTE: This requirement is subject to review once Annex K is available.

764 [\[RQ-DATA-1-03\]](#) The product shall prevent modification of configuration and firmware without authorization.

765 [\[RQ-DATA-1-04\]](#) The product shall restrict data processing and retention to the minimum that is required for its
766 intended functions.

767 5.7 Availability protection

768 5.7.1 General

769 This clause establishes requirements for protecting the availability of essential product functions during and after
770 security incidents. Products shall detect, withstand, and recover from denial-of-service attacks while preserving security
771 enforcement.

772 5.7.2 Requirements

773 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (h).

774 [\[RQ-AVAIL-1-01\]](#) The product shall enforce rate limiting for each network protocol terminated by the product.

775 [\[RQ-AVAIL-1-02\]](#) The product shall enforce connection throttling for each connection-oriented network protocol
776 terminated by the product.

777 [\[RQ-AVAIL-1-03\]](#) The product shall automatically recover when DoS conditions cease, without requiring manual
778 intervention.

779 5.8 Impact minimisation

780 5.8.1 General

781 This clause establishes requirements for minimising the negative impact of the product on the availability of services
782 provided by other products or networks. Products operating inline with network traffic can disrupt dependent systems
783 through excessive resource consumption or uncontrolled failure modes.

784 5.8.2 Requirements

785 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (i).

786 [\[RQ-IM-1-01\]](#) The product shall generate audit events when (i) resource utilization exceeds the documented high
787 utilization threshold and (ii) resource utilization returns below the documented high utilization threshold.

788 NOTE: The high utilization threshold levels are an implementation option and may be set by the manufacturer or
789 be available as a user-configurable setting.

790 5.9 Attack surface and mitigation

791 5.9.1 [INTEGRITY-1] System integrity and boot process

792 5.9.1.1 General

793 This clause establishes requirements for product integrity throughout the operational lifecycle, from initial power-on
794 through runtime operation. System integrity is the foundational trust anchor on which all other security controls depend.
795 A compromised boot process or runtime environment can subvert authentication, bypass access controls, and grant
796 persistent access without authorization that survives reboots and firmware updates.

797 The boot process is a critical attack surface for persistent implants, security control bypass, and extraction of
798 cryptographic material. Products operate autonomously for extended periods and control critical security functions.
799 Boot integrity and runtime security prevent attacks that could compromise entire network segments.

800 5.9.1.2 Requirements

801 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (k).

802 [\[RQ-INTEGRITY-1-01\]](#) The product shall verify boot component integrity using state of the art cryptography.

803 NOTE: This requirement is subject to review once Annex K is available.

804 [\[RQ-INTEGRITY-1-02\]](#) The product shall enforce a secure boot chain where (i) each stage verifies the next stage
805 before transferring control; (ii) the initial bootloader is immutable or hardware-protected; (iii) the product enters a
806 predefined failure state on verification failure; and (iv) only verified code executes during boot.

807 [\[RO-INTEGRITY-1-03\]](#) The product shall generate audit events for all boot events including (i) boot stage progression;
 808 (ii) verification, either success or failure, for each component; (iii) recovery mode activation; and (iv) detected bypass
 809 attempts.

810 NOTE: The generation of audit events at booting phases has constraints as the corresponding functionalities are
 811 not operational at this stage. An integrity error through these early phases is constrained by the absence of
 812 essential components and causes execution to halt or triggers a hard reset. As a consequence, audit events
 813 for such early errors cannot be generated as no memory is yet available for writing.

814 [\[RO-INTEGRITY-1-04\]](#) Where recovery or maintenance modes are present, the product shall require authentication
 815 and authorization before granting access to those modes.

816 5.9.2 [PACKET-1] Default packet disposition

817 5.9.2.1 General

818 These products differ fundamentally from general network infrastructure. Their primary purpose is security
 819 enforcement, not connectivity. The default-deny stance is their core operational principle. Products shall block traffic
 820 unless it has been explicitly validated. This applies even during resource exhaustion, parsing failures, or other
 821 exceptional conditions.

822 5.9.2.2 Requirements

823 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (j).

824 [\[RO-PACKET-1-01\]](#) Where the product cannot inspect traffic, the product shall apply the fail-secure action to that
 825 traffic.

826 [\[RO-PACKET-1-02\]](#) The product shall enable fail-open operation only through management override.

827 [\[RO-PACKET-1-03\]](#) Where stateful inspection is active, the product shall drop packets (i) that violate expected
 828 protocol state transitions; or (ii) that the product cannot reassemble for inspection.

829 NOTE: This requirement applies to network-layer stateful inspection.

830 [\[RO-PACKET-1-04\]](#) The product shall (i) generate security events; (ii) increment bypass counters; and (iii) block the
 831 traffic where explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

832 [\[RO-PACKET-1-05\]](#) The product shall drop packets that violate applicable protocol standards.

833 5.9.3 [EXPOSURE-1] Interface and service exposure minimization

834 5.9.3.1 General

835 This clause establishes requirements to limit exposed interfaces and services. Products shall expose only what their
 836 intended operation requires. Each exposed interface is an attack vector; reducing unnecessary exposure reduces risk.

837 5.9.3.2 Requirements

838 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (j).

839 [\[RO-EXPOSURE-1-01\]](#) The product, in its product operational state, shall enable only those interfaces and services that
 840 the intended function of the product requires.

841 [\[RO-EXPOSURE-1-02\]](#) The product shall provide capability to selectively enable or disable individual services and
 842 interfaces through configuration.

843 5.10 Monitoring and logging

844 5.10.1 General

845 This clause covers requirements for recording and monitoring. These products serve as primary sensors in security
 846 architectures. Records support incident detection, threat response, forensic analysis, and compliance checks. The
 847 following activities are logged: authentication attempts, configuration changes, threat detections, blocked attacks, and
 848 management actions. Event data is protected against modification or deletion without authorization.

849 5.10.2 Requirements

850 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (l).

851 [\[RQ-LOG-1-01\]](#) The product shall generate audit events for authentication activities including but not limited to (i)
852 successful or failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change
853 attempts.

854 [\[RQ-LOG-1-02\]](#) The product shall generate audit events for all session lifecycle activities including (i) session
855 establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv)
856 concurrent session limit violations.

857 [\[RQ-LOG-1-03\]](#) When a command is executed without authorization, the product shall generate an audit event.

858 5.11 Data management

859 5.11.1 [TRANSFER-1] Secure data export and transfer

860 5.11.1.1 General

861 This clause addresses secure data transfer between products. Users require the ability to migrate configurations,
862 operational data, and system state without loss of security. Configuration files contain critical security parameters and
863 need protection during export and transfer.

864 NOTE: This does not limit the choice of users to import data using legacy protocols maintained for backward
865 compatibility.

866 5.11.1.2 Requirements

867 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2) (m).

868 [\[RQ-TRANSFER-1-01\]](#) The product shall transfer exported and imported data over a secure channel.

869 NOTE: This requirement is subject to review once Annex K is available.

870 [\[RQ-TRANSFER-1-02\]](#) The product shall provide capability to export encrypted data using state of the art
871 cryptography, with encryption that is applied based on user preference.

872 NOTE: This requirement is subject to review once Annex K is available.

873 [\[RQ-TRANSFER-1-03\]](#) The product shall require management access for data export and data import operations.

874 [\[RQ-TRANSFER-1-04\]](#) The product shall generate audit events for all data export and data import operations.

875 5.11.2 [SIGNATURE-1] Signature update and validation

876 5.11.2.1 General

877 This clause covers signature database retrieval, validation, and application. Compromised or outdated signatures can
878 disable detection or introduce false negatives. The product shall maintain signature integrity and support secure
879 distribution.

880 5.11.2.2 Requirements

881 This clause addresses the requirements in the CRA [\[i.1\]](#), Annex I, Part I (2).

882 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-01] applies.

883 [\[RQ-SIGNATURE-1-01\]](#) The product shall verify signature database update integrity using state of the art
884 cryptography before installation.

885 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-02] applies.

886 [\[RQ-SIGNATURE-1-02\]](#) The product shall verify signature database integrity using state of the art cryptography before
887 use.

- 888 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-03] applies.
- 889 [\[RQ-SIGNATURE-1-03\]](#) The product shall prevent installation of signature database versions older than the currently
890 installed version.
- 891 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-04] applies.
- 892 [\[RQ-SIGNATURE-1-04\]](#) The product shall restore the signature database from backup when integrity verification fails.
- 893 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-05] applies.
- 894 [\[RQ-SIGNATURE-1-05\]](#) The product shall preserve user-created signatures when installing manufacturer-supplied
895 signature database updates.
- 896 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-06] applies.
- 897 [\[RQ-SIGNATURE-1-06\]](#) The product shall check for signature database updates at configurable intervals.
- 898 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-07] applies.
- 899 [\[RQ-SIGNATURE-1-07\]](#) The product shall defer signature database updates outside configured maintenance windows.
- 900 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-08] applies.
- 901 [\[RQ-SIGNATURE-1-08\]](#) The product shall limit signature database update download bandwidth to configurable
902 thresholds.
- 903 Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [RQ-SIGNATURE-1-09] applies.
- 904 [\[RQ-SIGNATURE-1-09\]](#) The product shall retry failed signature database downloads within 24 hours.

905 5.12 Remote data processing solutions

906 5.12.1 General

907 This clause establishes requirements for products that depend on remote data processing solutions as defined in Article
908 3, point 2, of Regulation (EU) 2024/2847. For firewalls, intrusion detection systems, and intrusion prevention systems,
909 RDPS dependencies commonly arise from cloud-based management, threat intelligence feeds, signature distribution,
910 and log collection services. Compromise of RDPS connectivity or authentication can disable security functions, inject
911 rules without authorization, poison threat intelligence, or expose protected data.

912 5.12.2 Requirements

- 913 Where risk factor [RF-RDPS-01] is present, requirement [RQ-RDPS-1-01] applies.
- 914 [\[RQ-RDPS-1-01\]](#) The manufacturer shall document all remote data processing solutions on which the product depends.
- 915 Where risk factor [RF-RDPS-01] is present, requirement [RQ-RDPS-1-02] applies.
- 916 [\[RQ-RDPS-1-02\]](#) Where the product communicates with a remote data processing solution, the product shall protect
917 that communication over a secure channel.
- 918 Where risk factor [RF-RDPS-01] is present, requirement [RQ-RDPS-1-03] applies.
- 919 [\[RQ-RDPS-1-03\]](#) Where the product communicates with a remote data processing solution, the product shall
920 authenticate the remote data processing solution before transmitting data to it.
- 921 Where risk factor [RF-RDPS-01] is present, requirement [RQ-RDPS-1-04] applies.
- 922 [\[RQ-RDPS-1-04\]](#) Where the product communicates with a remote data processing solution, the product shall retry
923 failed communications with the remote data processing solution within 24 hours.
- 924 Where risk factor [RF-RDPS-01] is present, requirement [RQ-RDPS-1-05] applies.
- 925 [\[RQ-RDPS-1-05\]](#) The product shall generate audit events for communication failures with a remote data processing
926 solution.

927

928 6 Assessment criteria for compliance with technical 929 requirements

930 6.1 Introduction

931 This clause details the assessment process for compliance with the requirements in clause [5](#) of the present document.

932 NOTE: In the following clauses, *documentation* means any documentation provided to the assessor. This
933 includes, but is not limited to, the technical specification, test results, and instructions to the user.

934 6.2 No known exploitable vulnerabilities

935 6.2.1 [KEV-1] No known exploitable vulnerabilities

936 6.2.1.1 Requirement assessments

937 [\[AC-KEV-1-01\]](#) Verify that the manufacturer maintains a software bill of materials for each product version in a
938 machine-readable format.

939 **Assessment reference**

940 Requirement [\[RO-KEV-1-01\]](#).

941 **Assessment objective**

942 Confirm that the manufacturer maintains a software bill of materials whose declared version matches the installed
943 version reported by the product.

944 **Assessment preparation**

- 945 1. The product is in product operational state.
- 946 2. The software bill of materials for the product is available.
- 947 3. Documentation describing the software bill of materials maintenance process is available.

948 **Assessment activities**

- 949 1. Review documentation to identify the software bill of materials maintenance process.
- 950 2. Inspect the software bill of materials and the installed version reported by the product. Verify that the version
951 declared in the software bill of materials matches the installed version reported by the product.

952 **Assessment verdict**

953 The verdict fail is assigned if any of the following conditions apply:

- 954 1. Documentation does not describe the software bill of materials maintenance process.
- 955 2. The manufacturer does not maintain a software bill of materials whose declared version matches the installed
956 version reported by the product.

957 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 958 1. Documentation describes the software bill of materials maintenance process.
- 959 2. The manufacturer maintains a software bill of materials whose declared version matches the installed version
960 reported by the product.

961 **Assessment evidence**

- 962 1. Documentation describing the software bill of materials maintenance process.
- 963 2. The software bill of materials and the installed version reported by the product.

964

965 [\[AC-KEV-1-02\]](#) Verify that the product contains no known exploitable vulnerabilities in each product version when
966 made available on the market.

967 **Assessment reference**

968 Requirement [\[RO-KEV-1-02\]](#).

969 **Assessment objective**

970 Confirm that no component of the product contains a known exploitable vulnerability in each product version when
971 made available on the market.

972 **Assessment preparation**

- 973 1. The product is in product factory default state.
- 974 2. Documentation describing the vulnerability assessment process is available.
- 975 3. The software bill of materials is available.

976 **Assessment activities**

- 977 1. Review the software bill of materials. Verify that all product components and third-party dependencies are
978 listed with version identifiers.
- 979 2. Cross-reference each component in the software bill of materials against known vulnerability databases. Verify
980 that no listed component has a known exploitable vulnerability at the time of assessment.
- 981 3. Verify that the software bill of materials is maintained in a machine-readable format.

982 **Assessment verdict**

983 The verdict fail is assigned if any of the following conditions apply:

- 984 1. The product does not provide a software bill of materials that lists all product components and third-party
985 dependencies with version identifiers.
- 986 2. The product contains a known exploitable vulnerability in one or more components listed in the software bill
987 of materials.
- 988 3. The product does not provide a software bill of materials in a machine-readable format.

989 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 990 1. The product provides a software bill of materials that lists all product components and third-party
991 dependencies with version identifiers.
- 992 2. The product does not contain a known exploitable vulnerability in any component listed in the software bill of
993 materials.
- 994 3. The product provides a software bill of materials in a machine-readable format.

995 **Assessment evidence**

- 996 1. Documentation showing the software bill of materials lists all product components and third-party
997 dependencies with version identifiers.
- 998 2. Test results showing no component listed in the software bill of materials contains a known exploitable
999 vulnerability.
- 1000 3. Documentation showing the format of the software bill of materials.

1001

1002 [\[AC-KEV-1-03\]](#) Verify that the manufacturer verifies third-party components against known vulnerability databases
1003 before making each product version available on the market.

1004 **Assessment reference**

1005 Requirement [\[RO-KEV-1-03\]](#).

1006 **Assessment objective**

1007 Confirm that the manufacturer verifies third-party components against known vulnerability databases before each
1008 release.

1009 **Assessment preparation**

- 1010 1. Documentation describing the third-party component verification process is available.
- 1011 2. The software bill of materials is available.

1012 **Assessment activities**

- 1013 1. Review documentation to identify the process for verifying third-party components against vulnerability
1014 databases before making each product version available on the market.
1015 2. Inspect the software bill of materials and verify that each third-party component is listed with a version
1016 identifier and has been checked against vulnerability databases.

1017 **Assessment verdict**

1018 The verdict fail is assigned if any of the following conditions apply:

- 1019 1. Documentation does not describe the third-party component verification process.
1020 2. Any third-party component lacks a version identifier or has not been verified against vulnerability databases.

1021 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1022 1. Documentation describes the third-party component verification process.
1023 2. All third-party components are listed with version identifiers and verified against vulnerability databases.

1024 **Assessment evidence**

- 1025 1. Documentation describing the third-party component verification process.
1026 2. Test results showing all third-party components are listed with version identifiers and verified against
1027 vulnerability databases.
1028

1029 **6.3 Secure by default configuration**

1030 **6.3.1 [DEFAULT-1] Secure by default configuration**

1031 **6.3.1.1 Requirement assessments**

1032 [\[AC-DEFAULT-1-01\]](#) Verify that the product enforces the applicable requirements of the present document in product
1033 factory default state, and that each excepted requirement (i) renders the initial product setup process non-functional; and
1034 (ii) the instructions to the user document the exception.

1035 **Assessment reference**

1036 Requirement [\[RO-DEFAULT-1-01\]](#).

1037 **Assessment objective**

1038 Confirm that the product enforces the applicable requirements of the present document in product factory default state,
1039 and that each excepted requirement (i) renders the initial product setup process non-functional; and (ii) the instructions
1040 to the user document the exception.

1041 **Assessment preparation**

- 1042 1. The product is in product factory default state.
1043 2. Documentation listing applicable requirements and their conformance status in product factory default state is
1044 available.
1045 3. Instructions to the user are available.

1046 **Assessment activities**

- 1047 1. Review documentation to identify the applicable requirements that are excepted from product factory default
1048 state.
1049 2. Review documentation for each excepted requirement to confirm the stated justification that conforming to it
1050 renders the initial product setup process non-functional.
1051 3. Inspect the product in product factory default state to identify all requirements that are not conformed to.
1052 Verify that each non-conformed requirement is listed in documentation as excepted.
1053 4. Inspect the product in product factory default state to verify that all non-excepted requirements are conformed
1054 to.
1055 5. Enforce conformance to each excepted requirement individually and attempt setup. Verify that setup fails.
1056 6. Review instructions to the user to verify that each excepted requirement is listed.

1057 **Assessment verdict**

1058 The verdict fail is assigned if any of the following conditions apply:

- 1059 1. Documentation does not list all applicable requirements excepted from product factory default state.
- 1060 2. Documentation does not describe the justification that conforming to each excepted requirement renders the
- 1061 initial product setup process non-functional.
- 1062 3. The product does not document any non-conformed requirement in product factory default state as excepted.
- 1063 4. Any non-excepted requirement is not conformed to in product factory default state.
- 1064 5. The product does not fail setup when any excepted requirement is individually enforced.
- 1065 6. Instructions to the user do not document every excepted requirement.

1066 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1067 1. Documentation lists all applicable requirements excepted from product factory default state.
- 1068 2. Documentation describes the justification that conforming to each excepted requirement renders the initial
- 1069 product setup process non-functional.
- 1070 3. The product documents every non-conformed requirement in product factory default state as excepted.
- 1071 4. All non-excepted requirements are conformed to in product factory default state.
- 1072 5. The product fails setup when each excepted requirement is individually enforced.
- 1073 6. Instructions to the user document every excepted requirement.

1074 **Assessment evidence**

- 1075 1. Documentation listing all applicable requirements excepted from product factory default state.
- 1076 2. Documentation describing the justification that conforming to each excepted requirement renders the initial
- 1077 product setup process non-functional.
- 1078 3. Test results showing the product documents every non-conformed requirement in product factory default state
- 1079 as excepted.
- 1080 4. Test results showing all non-excepted requirements are conformed to in product factory default state.
- 1081 5. Test results showing setup failure when each excepted requirement is individually enforced.
- 1082 6. Instructions to the user listing all excepted requirements.

1083

1084 [\[AC-DEFAULT-1-03\]](#) Verify that the product enforces all applicable requirements of the present document in product
1085 operational state.

1086 **Assessment reference**

1087 Requirement [\[RQ-DEFAULT-1-03\]](#).

1088 **Assessment objective**

1089 Confirm that the product enforces all applicable requirements of the present document in product operational state.

1090 **Assessment preparation**

- 1091 1. The product is in product operational state with initial setup complete.
- 1092 2. Documentation listing applicable requirements is available.

1093 **Assessment activities**

- 1094 1. Review documentation to identify all applicable requirements of the present document for product operational
- 1095 state.
- 1096 2. Inspect the product in product operational state to verify that all applicable requirements of the present
- 1097 document are conformed to.

1098 **Assessment verdict**

1099 The verdict fail is assigned if any of the following conditions apply:

- 1100 1. Documentation does not list all applicable requirements for product operational state.
- 1101 2. Any applicable requirement of the present document is not conformed to in product operational state.

1102 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1103 1. Documentation lists all applicable requirements for product operational state.
- 1104 2. All applicable requirements of the present document are conformed to in product operational state.

1105 **Assessment evidence**

- 1106 1. Documentation listing all applicable requirements for product operational state.
 1107 2. Test results showing all applicable requirements are conformed to in product operational state.
 1108

1109 [\[AC-DEFAULT-1-02\]](#) Verify that the product, in its product factory default state, enables only those interfaces and
 1110 services that product setup requires.

1111 **Assessment reference**

1112 Requirement [\[RO-DEFAULT-1-02\]](#).

1113 **Assessment objective**

1114 Confirm that the product enables only the interfaces and services that product setup requires in product factory default
 1115 state, and that no additional interfaces or services are active.

1116 **Assessment preparation**

- 1117 1. The product is in product factory default state.
 1118 2. Documentation describing the network interfaces and services required for product setup is available.

1119 **Assessment activities**

- 1120 1. Review documentation to identify all network interfaces and services required for product setup.
 1121 2. Inspect the product in product factory default state. Verify the product enables only network interfaces and
 1122 services documented as required for setup and does not initiate undocumented outbound connections.
 1123 3. Complete the product setup process using only the documented interfaces and services. Verify that setup
 1124 succeeds.
 1125 4. Attempt to access a network interface or service not documented as required for setup in product factory
 1126 default state. Verify that access is denied or the interface is inactive.

1127 **Assessment verdict**

1128 The verdict fail is assigned if any of the following conditions apply:

- 1129 1. Documentation does not list all interfaces and services required for product setup.
 1130 2. Any active network interface in product factory default state is not documented as required for setup.
 1131 3. Any listening network service in product factory default state is not documented as required for setup.
 1132 4. The product initiates an undocumented outbound connection in product factory default state.
 1133 5. The product does not complete setup successfully using only documented interfaces and services.
 1134 6. The product does not deny access to network interfaces and services not required for setup in product factory
 1135 default state.

1136 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1137 1. Documentation lists all interfaces and services required for product setup.
 1138 2. All active network interfaces in product factory default state are documented as required for setup.
 1139 3. All listening network services in product factory default state are documented as required for setup.
 1140 4. The product does not initiate any undocumented outbound connection in product factory default state.
 1141 5. The product completes setup successfully using only documented interfaces and services.
 1142 6. The product denies access to network interfaces and services not required for setup in product factory default
 1143 state.

1144 **Assessment evidence**

- 1145 1. Documentation listing all interfaces and services required for product setup.
 1146 2. Test results showing all active network interfaces in product factory default state are documented as required
 1147 for setup.
 1148 3. Test results showing all listening network services in product factory default state are documented as required
 1149 for setup.
 1150 4. Test results showing the product does not initiate any undocumented outbound connection in product factory
 1151 default state.
 1152 5. Test results showing setup completes successfully using only documented interfaces and services.

1153 6. Test results showing non-setup network interfaces and services are inaccessible in product factory default state.
1154

1155 [\[AC-DEFAULT-1-04\]](#) Verify that the product, in its product factory default state, restricts access to accounts and
1156 access methods documented in the instructions to the user.

1157 **Assessment reference**

1158 Requirement [\[RQ-DEFAULT-1-04\]](#).

1159 **Assessment objective**

1160 Confirm that the product restricts access to accounts and access methods documented in the instructions to the user, and
1161 that no undocumented accounts or access methods exist.

1162 **Assessment preparation**

- 1163 1. The product is in product factory default state.
- 1164 2. Instructions to the user describing factory default accounts and access methods are available.

1165 **Assessment activities**

- 1166 1. Review instructions to the user to identify all factory default accounts and access methods.
- 1167 2. Attempt access using each account and access method documented in the instructions to the user. Verify that
1168 access is granted.
- 1169 3. Attempt access using accounts and access methods not documented in the instructions to the user. Verify that
1170 the product restricts access by denying undocumented accounts.

1171 **Assessment verdict**

1172 The verdict fail is assigned if any of the following conditions apply:

- 1173 1. Instructions to the user do not identify all factory default accounts and access methods.
- 1174 2. Any account and access method documented in the instructions to the user is not functional in product factory
1175 default state.
- 1176 3. The product does not deny access using undocumented accounts and access methods.

1177 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1178 1. Instructions to the user identify all factory default accounts and access methods.
- 1179 2. All accounts and access methods documented in the instructions to the user are functional in product factory
1180 default state.
- 1181 3. The product denies access using undocumented accounts and access methods.

1182 **Assessment evidence**

- 1183 1. Instructions to the user listing all factory default accounts and access methods.
- 1184 2. Test results showing all accounts and access methods documented in the instructions to the user are functional
1185 in product factory default state.
- 1186 3. Test results showing undocumented accounts and access methods are denied.
1187

1188 [\[AC-DEFAULT-1-05\]](#) Verify that the product, in its product operational state, restricts access to accounts and
1189 authentication methods explicitly configured by the user.

1190 **Assessment reference**

1191 Requirement [\[RQ-DEFAULT-1-05\]](#).

1192 **Assessment objective**

1193 Confirm that the product does not provide access through accounts or authentication methods that were not explicitly
1194 configured, and that no undocumented or residual accounts exist in product operational state.

1195 **Assessment preparation**

- 1196 1. The product is in product operational state with at least one management account configured by the user.
- 1197 2. Documentation describing account management capabilities is available.

1198 **Assessment activities**

- 1199 1. Review documentation to identify account management capabilities and confirm that the product supports
1200 explicit configuration of accounts and authentication methods.
- 1201 2. Attempt access using each account and authentication method configured by the user. Verify that access is
1202 granted.
- 1203 3. Attempt access using accounts and authentication methods not configured by the user. Verify that the product
1204 denies access.

1205 **Assessment verdict**

1206 The verdict fail is assigned if any of the following conditions apply:

- 1207 1. Documentation does not describe account management capabilities.
- 1208 2. Documentation does not describe explicit configuration of accounts and authentication methods.
- 1209 3. Any account or authentication method configured by the user is not functional in product operational state.
- 1210 4. The product does not deny access using accounts and authentication methods not configured by the user.

1211 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1212 1. Documentation describes account management capabilities.
- 1213 2. Documentation describes explicit configuration of accounts and authentication methods.
- 1214 3. All accounts and authentication methods configured by the user are functional in product operational state.
- 1215 4. The product denies access using accounts and authentication methods not configured by the user.

1216 **Assessment evidence**

- 1217 1. Documentation describing account management capabilities.
- 1218 2. Documentation describing explicit configuration of accounts and authentication methods.
- 1219 3. Test results showing all configured accounts and authentication methods are functional.
- 1220 4. Test results showing accounts and authentication methods not configured by the user are denied.
- 1221

1222 [\[AC-DEFAULT-1-06\]](#) For credentials that are documented in the instructions to the user, verify that the product
1223 enforces change of those credentials in factory default state.

1224 **Assessment reference**

1225 Requirement [\[RQ-DEFAULT-1-06\]](#).

1226 **Assessment objective**

1227 For credentials that are documented in the instructions to the user, confirm that the product enforces change of those
1228 credentials before granting access to the product, and that this enforcement cannot be bypassed.

1229 **Assessment preparation**

- 1230 1. The product is in product factory default state with default credentials.
- 1231 2. Documentation describing default credential handling is available.

1232 **Assessment activities**

- 1233 1. Review documentation to identify the credential change process and requirements.
- 1234 2. Authenticate using factory default credentials. Verify that the product presents a credential change requirement
1235 before granting access to the product.
- 1236 3. Authenticate using factory default credentials to (i) trigger the credential change prompt; (ii) dismiss or bypass
1237 the prompt without completing the change; and (iii) attempt to access the product. Verify that access is denied.
- 1238 4. Record the factory default credentials from documentation and attempt to authenticate using those recorded
1239 credentials after completing the credential change. Verify that the original default credentials are rejected.

1240 **Assessment verdict**

1241 The verdict fail is assigned if any of the following conditions apply:

- 1242 1. Documentation does not describe the credential change process.
- 1243 2. The product does not enforce credential change on first access.

- 1244 3. The product does not deny access to the product when the credential change prompt is dismissed or bypassed
 1245 without completing the change.
 1246 4. The product does not reject original default credentials after the credential change.

1247 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1248 1. Documentation describes the credential change process.
 1249 2. The product enforces credential change on first access.
 1250 3. The product denies access to the product when the credential change prompt is dismissed or bypassed without
 1251 completing the change.
 1252 4. The product rejects original default credentials after the credential change.

1253 **Assessment evidence**

- 1254 1. Documentation describing the credential change process.
 1255 2. Test results showing the product enforces credential change on first access.
 1256 3. Test results showing the product denies access to the product when the credential change prompt is dismissed
 1257 or bypassed.
 1258 4. Test results showing default credentials are rejected after the credential change.
 1259

1260 [\[AC-DEFAULT-1-07\]](#) Verify that the product disables all diagnostic interfaces by default and protects any configurable
 1261 diagnostic interface with authentication and authorization.

1262 **Assessment reference**

1263 Requirement [\[RQ-DEFAULT-1-07\]](#).

1264 **Assessment objective**

1265 Confirm that all diagnostic interfaces are disabled by default, and that where the product provides configuration to
 1266 enable a diagnostic interface, that interface requires authentication and authorization.

1267 **Assessment preparation**

- 1268 1. The product is in product factory default state.
 1269 2. Documentation listing all debugging and diagnostic interfaces is available.

1270 **Assessment activities**

- 1271 1. Review documentation to identify all debugging and diagnostic interfaces.
 1272 2. Inspect the product in product factory default state to identify all debugging and diagnostic interfaces. Verify
 1273 that each is disabled.
 1274 3. Attempt to access each documented debugging and diagnostic interface. Verify that access is denied or the
 1275 interface is inactive.
 1276 4. Enable a configurable diagnostic interface where the product provides configuration to do so. Attempt to
 1277 access the enabled diagnostic interface without authentication. Verify that the product denies access.
 1278 5. Attempt to access the enabled diagnostic interface without authorization. Verify that the product denies access.
 1279 6. Authenticate and authorize access to the enabled diagnostic interface. Verify that access is granted.

1280 **Assessment verdict**

1281 The verdict fail is assigned if any of the following conditions apply:

- 1282 1. Documentation does not list all debugging and diagnostic interfaces.
 1283 2. Any debugging or diagnostic interface is enabled in product factory default state.
 1284 3. Any documented debugging or diagnostic interface does not deny access in product factory default state.
 1285 4. The product does not deny access to the enabled diagnostic interface without authentication.
 1286 5. The product does not deny access to the enabled diagnostic interface without authorization.
 1287 6. The product does not grant access to the enabled diagnostic interface with authentication and authorization.

1288 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1289 1. Documentation lists all debugging and diagnostic interfaces.
 1290 2. All debugging and diagnostic interfaces are disabled in product factory default state.
 1291 3. All documented debugging and diagnostic interfaces deny access in product factory default state.

- 1292 4. The product denies access to the enabled diagnostic interface without authentication.
 1293 5. The product denies access to the enabled diagnostic interface without authorization.
 1294 6. The product grants access to the enabled diagnostic interface with authentication and authorization.

1295 **Assessment evidence**

- 1296 1. Documentation listing all debugging and diagnostic interfaces.
 1297 2. Test results showing all debugging and diagnostic interfaces are disabled in factory default state.
 1298 3. Test results showing all documented debugging and diagnostic interfaces deny access in product factory
 1299 default state.
 1300 4. Test results showing the product denies access to the enabled diagnostic interface without authentication.
 1301 5. Test results showing the product denies access to the enabled diagnostic interface without authorization.
 1302 6. Test results showing the product grants access to the enabled diagnostic interface with authentication and
 1303 authorization.
 1304

1305 [\[AC-DEFAULT-1-08\]](#) Verify that the product generates audit events for product errors.

1306 **Assessment reference**

1307 Requirement [\[RQ-DEFAULT-1-08\]](#).

1308 **Assessment objective**

1309 Confirm that the product generates audit events for product errors.

1310 **Assessment preparation**

- 1311 1. The product is in product operational state.
 1312 2. Documentation describing product error audit events is available.

1313 **Assessment activities**

- 1314 1. Review documentation to identify the product error conditions that generate audit events.
 1315 2. Trigger a product error condition. Verify that the product generates an audit event for the product error.

1316 **Assessment verdict**

1317 The verdict fail is assigned if any of the following conditions apply:

- 1318 1. Documentation does not list the product error conditions that generate audit events.
 1319 2. The product does not generate an audit event for product errors.

1320 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1321 1. Documentation lists the product error conditions that generate audit events.
 1322 2. The product generates an audit event for product errors.

1323 **Assessment evidence**

- 1324 1. Documentation listing the product error conditions that generate audit events.
 1325 2. Test results showing the product generates an audit event for product errors.
 1326

1327 [\[AC-DEFAULT-1-09\]](#) Verify that the product requires state of the art cryptography for all cryptographic functions.

1328 **Assessment reference**

1329 Requirement [\[RQ-DEFAULT-1-09\]](#).

1330 **Assessment objective**

1331 Confirm that the product requires state of the art cryptography for all cryptographic functions, and that no deprecated or
 1332 weak cryptography is enabled.

1333 **Assessment preparation**

- 1334 1. Documentation describing the cryptographic configuration is available.

1335 **Assessment activities**

- 1336 1. Review documentation to identify the cryptographic configuration.
- 1337 2. Inspect the product in product factory default state to verify the active cryptographic configuration matches the
- 1338 documented cryptographic configuration and is state of the art.
- 1339 3. Inspect the product in product operational state to verify the active cryptographic configuration matches the
- 1340 documented cryptographic configuration and is state of the art.
- 1341 4. Verify that where cryptographic negotiation is supported, the default order does not prefer deprecated
- 1342 cryptography over recognized cryptography, and that where only fixed configuration is used, no negotiation
- 1343 occurs.

1344 **Assessment verdict**

1345 The verdict fail is assigned if any of the following conditions apply:

- 1346 1. Documentation does not describe the cryptographic configuration.
- 1347 2. The product does not use state of the art cryptography in product factory default state.
- 1348 3. The product does not use state of the art cryptography in product operational state.
- 1349 4. The product does not prioritize recognized cryptography over deprecated cryptography in the default
- 1350 negotiation order where negotiation is supported.
- 1351 5. The product performs cryptographic negotiation where only fixed configuration is used.

1352 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1353 1. Documentation describes the cryptographic configuration.
- 1354 2. The product uses state of the art cryptography in product factory default state.
- 1355 3. The product uses state of the art cryptography in product operational state.
- 1356 4. The product prioritizes recognized cryptography over deprecated cryptography in the default negotiation order
- 1357 where negotiation is supported.
- 1358 5. The product does not perform cryptographic negotiation where only fixed configuration is used.

1359 **Assessment evidence**

- 1360 1. Documentation describing the cryptographic configuration.
- 1361 2. Test results showing the cryptographic configuration is state of the art in product factory default state.
- 1362 3. Test results showing the cryptographic configuration is state of the art in product operational state.
- 1363 4. Test results showing the default negotiation order does not prefer deprecated cryptography over recognized
- 1364 cryptography where negotiation is supported.
- 1365 5. Test results showing no cryptographic negotiation occurs where only fixed configuration is used.
- 1366

1367 [\[AC-DEFAULT-1-10\]](#) Verify that the product does not support protocols with known exploitable vulnerabilities.

1368 **Assessment reference**

1369 Requirement [\[RQ-DEFAULT-1-10\]](#).

1370 **Assessment objective**

1371 Confirm that the product does not support any protocol with known exploitable vulnerabilities.

1372 **Assessment preparation**

- 1373 1. The product is in product operational state.
- 1374 2. Documentation describing protocols supported by the product is available.
- 1375 3. A current vulnerability database is accessible.

1376 **Assessment activities**

- 1377 1. Review documentation to identify all protocols supported by the product.
- 1378 2. Perform a protocol scan of the product. Verify no protocol with known exploitable vulnerabilities is present.

1379 **Assessment verdict**

1380 The verdict fail is assigned if any of the following conditions apply:

- 1381 1. Documentation does not list all protocols supported by the product.

1382 2. The product supports protocols with known exploitable vulnerabilities.

1383 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1384 1. Documentation lists all protocols supported by the product.

1385 2. The product does not support protocols with known exploitable vulnerabilities.

1386 **Assessment evidence**

1387 1. Documentation listing all protocols supported by the product.

1388 2. Test results showing the product does not support protocols with known exploitable vulnerabilities.

1389

1390 [\[AC-DEFAULT-1-11\]](#) Verify that the product enables mitigations for known design limitations of protocols terminated
1391 by the product.

1392 **Assessment reference**

1393 Requirement [\[RQ-DEFAULT-1-11\]](#).

1394 **Assessment objective**

1395 Confirm that the product enables mitigations for known design limitations of protocols terminated by the product, and
1396 that mitigations are enabled by default.

1397 **Assessment preparation**

1398 1. The product is in product operational state.

1399 2. Documentation describing all protocols terminated by the product is available.

1400 **Assessment activities**

1401 1. Review documentation to identify all protocols terminated by the product, their known design limitations, and
1402 the mitigations implemented for each.

1403 2. Scan the product to enumerate active protocols. Verify that each active protocol is documented.

1404 3. Verify that each documented mitigation is enabled by default.

1405 **Assessment verdict**

1406 The verdict fail is assigned if any of the following conditions apply:

1407 1. Documentation does not list all protocols terminated by the product, their known design limitations, and
1408 mitigations.

1409 2. Any active protocol terminated by the product is not documented.

1410 3. Any documented mitigation is not enabled by default.

1411 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1412 1. Documentation lists all protocols terminated by the product, their known design limitations, and mitigations.

1413 2. Each active protocol terminated by the product is documented.

1414 3. Each documented mitigation is enabled by default.

1415 **Assessment evidence**

1416 1. Documentation listing all protocols terminated by the product, their known design limitations, and mitigations.

1417 2. Test results showing each active protocol terminated by the product is documented.

1418 3. Test results showing each documented mitigation is enabled by default.

1419

1420 [\[AC-DEFAULT-1-12\]](#) Verify that the product enforces the principle of least privilege during normal operation.

1421 **Assessment reference**

1422 Requirement [\[RQ-DEFAULT-1-12\]](#).

1423 **Assessment objective**

1424 Confirm that the product enforces the principle of least privilege by defining distinct privilege levels, restricting each
1425 account to its assigned privileges, and preventing privilege escalation without authorization.

1426 **Assessment preparation**

- 1427 1. The product is in product operational state with initialization complete.
- 1428 2. Documentation describing the role and permission model is available.
- 1429 3. Accounts for each defined role are available or can be created.

1430 **Assessment activities**

- 1431 1. Review documentation to identify all defined roles and their assigned operations.
- 1432 2. Authenticate with an account of each defined role. Verify that all assigned operations are available.
- 1433 3. Authenticate with each defined role in turn and attempt operations assigned to a higher-privilege role. Verify that access is denied for each attempt.
- 1434 4. Attempt privilege escalation without authorization. Verify that the product rejects the attempt.
- 1435 5. Inspect running processes and services on the product where accessible to verify they run with minimum required privileges and not as root or equivalent unless documented as necessary.

1438 **Assessment verdict**

1439 The verdict fail is assigned if any of the following conditions apply:

- 1440 1. Documentation does not list all roles, their privilege levels, and assigned operations.
- 1441 2. Any defined role does not perform all its assigned operations.
- 1442 3. The product does not deny operations assigned to higher-privilege roles to lower-privilege accounts.
- 1443 4. The product does not reject privilege escalation attempts without authorization.
- 1444 5. The product does not run all inspected processes with minimum required privileges where process listing is accessible.

1446 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1447 1. Documentation lists all roles, their privilege levels, and assigned operations.
- 1448 2. Each defined role performs all its assigned operations.
- 1449 3. The product denies operations assigned to higher-privilege roles to lower-privilege accounts.
- 1450 4. The product rejects privilege escalation attempts without authorization.
- 1451 5. The product runs all inspected processes with minimum required privileges where process listing is accessible.

1452 **Assessment evidence**

- 1453 1. Documentation listing all roles, privilege levels, and assigned operations.
- 1454 2. Test results showing each defined role performs all its assigned operations.
- 1455 3. Test results showing the product denies operations assigned to higher-privilege roles to lower-privilege accounts.
- 1456 4. Test results showing the product rejects privilege escalation attempts without authorization.
- 1457 5. Test results showing the product runs all inspected processes with minimum required privileges where process listing is accessible.

1460

1461 [\[AC-DEFAULT-1-13\]](#) Verify that the product stores audit events in persistent memory that survives a reboot.

1462 **Assessment reference**

1463 Requirement [\[RQ-DEFAULT-1-13\]](#).

1464 **Assessment objective**

1465 Confirm that the product stores audit events in persistent memory that survives the reboot.

1466 **Assessment preparation**

- 1467 1. The product is in product operational state.
- 1468 2. Documentation describing audit event storage mechanisms is available.

1469 **Assessment activities**

- 1470 1. Review documentation to identify the audit event storage mechanism.
- 1471 2. Perform a reboot. Verify that audit events recorded before the reboot are present and intact after the reboot.

- 1472 3. Perform a power cycle. Verify that audit events recorded before the power cycle are present and intact after the
1473 power cycle.

1474 **Assessment verdict**

1475 The verdict fail is assigned if any of the following conditions apply:

- 1476 1. Documentation does not list the audit event storage mechanism.
1477 2. The product does not store audit events in persistent memory that survives a reboot.
1478 3. The product does not store audit events in persistent memory that survives a power cycle.

1479 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1480 1. Documentation lists the audit event storage mechanism.
1481 2. The product stores audit events in persistent memory that survives a reboot.
1482 3. The product stores audit events in persistent memory that survives a power cycle.

1483 **Assessment evidence**

- 1484 1. Documentation listing the audit event storage mechanism.
1485 2. Test results showing the product stores audit events in persistent memory that survives a reboot.
1486 3. Test results showing the product stores audit events in persistent memory that survives a power cycle.
1487

1488 **6.3.2 [RESET-1] Factory reset**

1489 **6.3.2.1 Requirement assessments**

1490 [\[AC-RESET-1-01\]](#) Verify that the product provides a factory reset mechanism that restores the product to its secure-by-
1491 default configuration.

1492 **Assessment reference**

1493 Requirement [\[RQ-RESET-1-01\]](#).

1494 **Assessment objective**

1495 Confirm that the product provides a factory reset mechanism that restores the product to its secure-by-default
1496 configuration.

1497 **Assessment preparation**

- 1498 1. The product is in product operational state.
1499 2. Documentation describing the factory reset mechanism and procedure is available.

1500 **Assessment activities**

- 1501 1. Review documentation to identify the factory reset mechanism and procedure. Verify the product provides a
1502 documented factory reset mechanism.
1503 2. Perform a factory reset. Verify that the product is restored to its secure-by-default configuration.
1504 3. Perform the assessments in clause [5.3.1](#) on the post-reset product. Verify that all assessments pass.

1505 **Assessment verdict**

1506 The verdict fail is assigned if any of the following conditions apply:

- 1507 1. Documentation does not describe the factory reset mechanism or procedure.
1508 2. The product does not restore its secure-by-default configuration after factory reset.
1509 3. The product does not pass all assessments in clause [5.3.1](#) after factory reset.

1510 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1511 1. Documentation describes the factory reset mechanism and procedure.
1512 2. The product restores its secure-by-default configuration after factory reset.
1513 3. The product passes all assessments in clause [5.3.1](#) after factory reset.

1514 **Assessment evidence**

- 1515 1. Documentation describing the factory reset mechanism and procedure.

- 1516 2. Test results showing the product is restored to its secure-by-default configuration after factory reset.
 1517 3. Test results showing the product passes all assessments in clause [5.3.1](#) after factory reset.

1518

1519 [\[AC-RESET-1-02\]](#) Verify that the product maintains the currently installed firmware version and all installed security
 1520 updates after factory reset.

1521 **Assessment reference**

1522 Requirement [\[RQ-RESET-1-02\]](#).

1523 **Assessment objective**

1524 Confirm that the product provides a factory reset mechanism that maintains the currently installed firmware version and
 1525 all installed security updates, without reverting to the firmware version when made available on the market.

1526 **Assessment preparation**

- 1527 1. The product is in product operational state with at least one security update applied beyond the firmware
 1528 version when made available on the market.
 1529 2. Documentation describing factory reset behaviour for firmware version and security updates is available.

1530 **Assessment activities**

- 1531 1. Review documentation to confirm the product provides a factory reset mechanism that preserves firmware
 1532 version and security updates.
 1533 2. Perform factory reset. Verify that the product maintains (i) the currently installed firmware version; and (ii) all
 1534 installed security updates.

1535 **Assessment verdict**

1536 The verdict fail is assigned if any of the following conditions apply:

- 1537 1. Documentation does not describe that factory reset preserves firmware version and installed security updates.
 1538 2. The product does not maintain the currently installed firmware version after factory reset.
 1539 3. Any installed security update does not remain applied after factory reset.

1540 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1541 1. Documentation describes that factory reset preserves firmware version and installed security updates.
 1542 2. The product maintains the currently installed firmware version after factory reset.
 1543 3. All installed security updates remain applied after factory reset.

1544 **Assessment evidence**

- 1545 1. Documentation describing factory reset behaviour for firmware and installed security updates.
 1546 2. Test results showing the product maintains the currently installed firmware version after factory reset.
 1547 3. Test results showing all installed security updates remain applied after factory reset.

1548

1549 [\[AC-RESET-1-03\]](#) Verify that the product does not retain (i) previous configuration; (ii) user data; or (iii) critical
 1550 security parameters after factory reset.

1551 **Assessment reference**

1552 Requirement [\[RQ-RESET-1-03\]](#).

1553 **Assessment objective**

1554 Confirm that the product does not retain (i) previous configuration; (ii) user data; or (iii) critical security parameters
 1555 after factory reset.

1556 **Assessment preparation**

- 1557 1. The product is in product operational state.
 1558 2. Documentation describing factory reset behaviour is available.

1559 **Assessment activities**

- 1560 1. Review documentation to identify data retained and data removed during factory reset.
 1561 2. Modify the product configuration, create user data, and configure critical security parameters. Verify the
 1562 modifications are present before factory reset.
 1563 3. Perform factory reset. Attempt to retrieve the previously modified configuration through the product.
 1564 4. Attempt to retrieve the previously created user data through the product after factory reset.
 1565 5. Attempt to retrieve the previously configured critical security parameters through the product after factory
 1566 reset.

1567 **Assessment verdict**

1568 The verdict fail is assigned if any of the following conditions apply:

- 1569 1. Documentation does not describe data retained and data removed during factory reset.
 1570 2. The product does not contain modified configuration, user data, or critical security parameters before factory
 1571 reset.
 1572 3. The product retains previous configuration after factory reset.
 1573 4. The product retains user data after factory reset.
 1574 5. The product retains critical security parameters after factory reset.

1575 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1576 1. Documentation describes data retained and data removed during factory reset.
 1577 2. The product contains modified configuration, user data, and critical security parameters before factory reset.
 1578 3. The product does not retain previous configuration after factory reset.
 1579 4. The product does not retain user data after factory reset.
 1580 5. The product does not retain critical security parameters after factory reset.

1581 **Assessment evidence**

- 1582 1. Documentation describing data retained and data removed during factory reset.
 1583 2. Test results showing the product contains modified configuration, user data, and critical security parameters
 1584 before factory reset.
 1585 3. Test results showing the product does not retain previous configuration after factory reset.
 1586 4. Test results showing the product does not retain user data after factory reset.
 1587 5. Test results showing the product does not retain critical security parameters after factory reset.
 1588

1589 **6.4 Secure updates**

1590 **6.4.1 [UPDATE-1] Update mechanisms**

1591 **6.4.1.1 Requirement assessments**

1592 [\[AC-UPDATE-1-01\]](#) Verify that the product provides a mechanism to receive security updates.

1593 **Assessment reference**

1594 Requirement [\[RO-UPDATE-1-01\]](#).

1595 **Assessment objective**

1596 Confirm that the product provides a mechanism to receive security updates through on-product delivery, off-the-product
 1597 delivery, or both.

1598 **Assessment preparation**

- 1599 1. The product is in product operational state.
 1600 2. Documentation describing the security update delivery method is available.

1601 **Assessment activities**

- 1602 1. Review documentation to identify whether the product supports on-product delivery, off-the-product delivery,
 1603 or both.

- 1604 2. Verify that the product downloads the security update through the on-product mechanism, where the product
1605 supports on-product delivery.
1606 3. Obtain a security update through the documented off-the-product procedure, where the product supports off-
1607 the-product delivery.

1608 **Assessment verdict**

1609 The verdict fail is assigned if any of the following conditions apply:

- 1610 1. Documentation does not describe the security update delivery method.
1611 2. The product does not download the security update through the on-product mechanism.
1612 3. The product does not provide a mechanism to receive security updates through the documented off-the-product
1613 procedure.

1614 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1615 1. Documentation describes the security update delivery method.
1616 2. The product downloads the security update through the on-product mechanism.
1617 3. The product provides a mechanism to receive security updates through the documented off-the-product
1618 procedure.

1619 **Assessment evidence**

- 1620 1. Documentation describing the security update delivery method.
1621 2. Test results showing the product downloads the security update through the on-product mechanism.
1622 3. Test results showing the product provides a mechanism to receive security updates through the off-the-product
1623 procedure.
1624

1625 [\[AC-UPDATE-1-02\]](#) Verify that the product prevents installation of security updates without authentication and
1626 without authorization.

1627 **Assessment reference**

1628 Requirement [\[RO-UPDATE-1-02\]](#).

1629 **Assessment objective**

1630 Confirm that the product prevents installation of security updates without authentication and without authorization.

1631 **Assessment preparation**

- 1632 1. The product is in product operational state.
1633 2. Documentation describing authentication and authorization requirements for security update installation is
1634 available.

1635 **Assessment activities**

- 1636 1. Review documentation to identify the authentication and authorization requirements for security update
1637 installation.
1638 2. Attempt to install a security update without authentication. Verify that the product prevents the installation.
1639 3. Attempt to install a security update without authorization. Verify that the product prevents the installation.

1640 **Assessment verdict**

1641 The verdict fail is assigned if any of the following conditions apply:

- 1642 1. Documentation does not describe the authentication and authorization requirements for security update
1643 installation.
1644 2. The product does not prevent security update installation without authentication.
1645 3. The product does not prevent security update installation without authorization.

1646 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1647 1. Documentation describes the authentication and authorization requirements for security update installation.
1648 2. The product prevents security update installation without authentication.
1649 3. The product prevents security update installation without authorization.

1650 **Assessment evidence**

- 1651 1. Documentation describing the authentication and authorization requirements for security update installation.
- 1652 2. Test results showing the product prevents security update installation without authentication.
- 1653 3. Test results showing the product prevents security update installation without authorization.

1654

1655 [\[AC-UPDATE-1-03\]](#) Verify that the product installs a received security update and reports the installed version.1656 **Assessment reference**1657 Requirement [\[RQ-UPDATE-1-03\]](#).1658 **Assessment objective**

1659 Confirm that the product installs a received security update and reports the installed version after installation.

1660 **Assessment preparation**

- 1661 1. The product is in product operational state.
- 1662 2. A security update has been received through the documented delivery method.

1663 **Assessment activities**

- 1664 1. Review documentation to identify the security update installation procedure and the version reporting mechanism.
- 1665
- 1666 2. Install the received security update. Verify that the product reports the installed version after installation.

1667 **Assessment verdict**

1668 The verdict fail is assigned if any of the following conditions apply:

- 1669 1. Documentation does not describe the security update installation procedure and the version reporting mechanism.
- 1670
- 1671 2. The product does not install the security update.
- 1672 3. The product does not report the installed version.

1673 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1674 1. Documentation describes the security update installation procedure and the version reporting mechanism.
- 1675 2. The product installs the security update.
- 1676 3. The product reports the installed version.

1677 **Assessment evidence**

- 1678 1. Documentation describing the security update installation procedure and the version reporting mechanism.
- 1679 2. Test results showing the product installs the security update.
- 1680 3. Test results showing the product reports the installed version.

1681

1682 [\[AC-UPDATE-1-04\]](#) Verify that the product retries failed security update delivery and installation attempts.1683 **Assessment reference**1684 Requirement [\[RQ-UPDATE-1-04\]](#).1685 **Assessment objective**

1686 Confirm that the product retries failed security update delivery and installation attempts.

1687 **Assessment preparation**

- 1688 1. The product is in product operational state.
- 1689 2. Documentation describing the retry behaviour is available.

1690 **Assessment activities**

- 1691 1. Review documentation to identify the retry behaviour for failed delivery and installation attempts.
- 1692 2. Initiate a security update delivery and cause it to fail. Verify that the product retries the delivery.

1693 3. Initiate a security update installation and cause it to fail. Verify that the product retries the installation.

1694 **Assessment verdict**

1695 The verdict fail is assigned if any of the following conditions apply:

- 1696 1. Documentation does not describe the retry behaviour for failed delivery and installation attempts.
- 1697 2. The product does not retry failed security update delivery.
- 1698 3. The product does not retry failed security update installation.

1699 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1700 1. Documentation describes the retry behaviour for failed delivery and installation attempts.
- 1701 2. The product retries failed security update delivery.
- 1702 3. The product retries failed security update installation.

1703 **Assessment evidence**

- 1704 1. Documentation describing the retry behaviour for failed delivery and installation attempts.
- 1705 2. Test results showing the product retries failed security update delivery.
- 1706 3. Test results showing the product retries failed security update installation.

1707

1708 [\[AC-UPDATE-1-05\]](#) Verify that where the product supports on-product delivery, the product enables by default an
1709 automated mechanism that detects available security updates.

1710 **Assessment reference**

1711 Requirement [\[RQ-UPDATE-1-05\]](#).

1712 **Assessment objective**

1713 Confirm that where the product supports on-product delivery, the product enables by default an automated mechanism
1714 that detects available security updates.

1715 **Assessment preparation**

- 1716 1. The product is in product operational state.
- 1717 2. Documentation describing the automated security update detection mechanism is available.

1718 **Assessment activities**

- 1719 1. Review documentation to identify the automated security update detection mechanism.
- 1720 2. Inspect the product in product operational state. Verify that the automated security update detection
1721 mechanism is enabled by default.

1722 **Assessment verdict**

1723 The verdict fail is assigned if any of the following conditions apply:

- 1724 1. Documentation does not describe the automated security update detection mechanism.
- 1725 2. The product does not enable the automated security update detection mechanism by default.

1726 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1727 1. Documentation describes the automated security update detection mechanism.
- 1728 2. The product enables the automated security update detection mechanism by default.

1729 **Assessment evidence**

- 1730 1. Documentation describing the automated security update detection mechanism.
- 1731 2. Test results showing the automated security update detection mechanism is enabled by default.

1732

1733 [\[AC-UPDATE-1-06\]](#) Verify that the product verifies security update integrity using state of the art cryptography before
1734 installation.

1735 **Assessment reference**

1736 Requirement [\[RQ-UPDATE-1-06\]](#).

1737 **Assessment objective**

1738 Confirm that the product verifies security update integrity using state of the art cryptography before installation.

1739 **Assessment preparation**

- 1740 1. The product is in product operational state.
- 1741 2. Documentation describing the security update integrity verification mechanism is available.

1742 **Assessment activities**

- 1743 1. Review documentation to identify the security update integrity verification mechanism.
- 1744 2. Inspect the documented security update verification mechanism. Verify the cryptography used is state of the art.
- 1745 1746 3. Install a valid security update. Verify the product performs cryptographic verification before installation proceeds.
- 1747 1748 4. Attempt to install a tampered security update. Verify that the product rejects the installation.

1749 **Assessment verdict**

1750 The verdict fail is assigned if any of the following conditions apply:

- 1751 1. Documentation does not describe the security update integrity verification mechanism.
- 1752 2. The product does not use state of the art cryptography for security update verification.
- 1753 3. The product does not perform cryptographic verification before installing the security update.
- 1754 4. The product does not reject installation of a tampered security update.

1755 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1756 1. Documentation describes the security update integrity verification mechanism.
- 1757 2. The product uses state of the art cryptography for security update verification.
- 1758 3. The product performs cryptographic verification before installing the security update.
- 1759 4. The product rejects installation of a tampered security update.

1760 **Assessment evidence**

- 1761 1. Documentation describing the security update integrity verification mechanism.
- 1762 2. Test results showing the security update verification uses state of the art cryptography.
- 1763 3. Test results showing the product performs cryptographic verification before installing the security update.
- 1764 4. Test results showing the product rejects installation of a tampered security update.

1765

1766 [\[AC-UPDATE-1-07\]](#) Verify that the product generates audit events for (i) security update availability; (ii) security
 1767 update download initiation, completion, or failure; and (iii) security update installation success or failure.

1768 **Assessment reference**1769 Requirement [\[RQ-UPDATE-1-07\]](#).1770 **Assessment objective**

1771 Confirm that the product generates audit events for (i) security update availability; (ii) security update download
 1772 initiation, completion, or failure; and (iii) security update installation success or failure.

1773 **Assessment preparation**

- 1774 1. The product is in product operational state.
- 1775 2. Documentation describing audit events generated for security update activities is available.

1776 **Assessment activities**

- 1777 1. Review documentation to identify the audit events generated for security update activities.
- 1778 2. Trigger a security update availability notification. Verify that the product generates an audit event for security
 1779 update availability.
- 1780 3. Initiate and complete a security update download. Verify that the product generates audit events for security
 1781 update download initiation, completion, or failure.

- 1782 4. Perform a security update installation. Verify that the product generates an audit event for security update
1783 installation success or failure.

1784 **Assessment verdict**

1785 The verdict fail is assigned if any of the following conditions apply:

- 1786 1. Documentation does not describe audit events for security update activities.
1787 2. The product does not generate an audit event for security update availability.
1788 3. The product does not generate audit events for security update download initiation, completion, or failure.
1789 4. The product does not generate an audit event for security update installation success or failure.

1790 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1791 1. Documentation describes audit events for security update activities.
1792 2. The product generates an audit event for security update availability.
1793 3. The product generates audit events for security update download initiation, completion, or failure.
1794 4. The product generates an audit event for security update installation success or failure.

1795 **Assessment evidence**

- 1796 1. Documentation describing audit events generated for security update activities.
1797 2. Test results showing the product generates an audit event for security update availability.
1798 3. Test results showing the product generates audit events for security update download initiation, completion, or
1799 failure.
1800 4. Test results showing the product generates an audit event for security update installation success or failure.
1801

1802 **6.5 Authentication and access control**

1803 **6.5.1 [AUTH-1] Authentication**

1804 **6.5.1.1 Requirement assessments**

1805 [\[AC-AUTH-1-01\]](#) Verify that the product requires user authentication on all interfaces providing access to the product.

1806 **Assessment reference**

1807 Requirement [\[RO-AUTH-1-01\]](#).

1808 **Assessment objective**

1809 Confirm that the product requires user authentication on all interfaces providing access to the product, and that access
1810 without authentication is denied.

1811 **Assessment preparation**

- 1812 1. The product is in product operational state.
1813 2. Documentation describing the user authentication mechanism is available.

1814 **Assessment activities**

- 1815 1. Review documentation to identify all authentication mechanisms and interfaces on which authentication is
1816 required.
1817 2. Attempt to access the product on each interface without providing credentials. Verify access is denied.
1818 3. Authenticate using valid credentials on each interface. Verify access is granted.
1819 4. Authenticate using valid credentials and perform a series of operations without re-authenticating. Verify the
1820 product maintains authentication state throughout the session without requiring repeated credential entry.
1821 5. Attempt to access the product on each interface with invalid credentials. Verify access is denied.

1822 **Assessment verdict**

1823 The verdict fail is assigned if any of the following conditions apply:

- 1824 1. Documentation does not describe the authentication mechanism, method, or interfaces requiring
1825 authentication.

- 1826 2. The product does not deny access without authentication on any interface.
 1827 3. The product does not grant access with valid credentials on any interface.
 1828 4. The product does not maintain authentication state throughout the session without requiring repeated credential
 1829 entry.
 1830 5. The product does not reject invalid credentials on any interface.

1831 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1832 1. Documentation describes the authentication mechanism, method, and all interfaces requiring authentication.
 1833 2. The product denies access without authentication on all interfaces.
 1834 3. The product grants access with valid credentials on each interface.
 1835 4. The product maintains authentication state throughout the session without requiring repeated credential entry.
 1836 5. The product rejects invalid credentials on each interface.

1837 **Assessment evidence**

- 1838 1. Documentation describing the authentication mechanism, method, and all interfaces requiring authentication.
 1839 2. Test results showing access without authentication is denied on each interface.
 1840 3. Test results showing valid credentials grant access on each interface.
 1841 4. Test results showing the product maintains authentication state throughout the session using valid credentials
 1842 without re-authenticating.
 1843 5. Test results showing the product rejects invalid credentials on each interface.
 1844

1845 [\[AC-AUTH-1-02\]](#) Verify that the product provides unique credentials per product unit during secure production.

1846 **Assessment reference**

1847 Requirement [\[RQ-AUTH-1-02\]](#).

1848 **Assessment objective**

1849 Confirm that the product provides unique credentials per product unit during secure production, and that no two product
 1850 units share default credentials.

1851 **Assessment preparation**

- 1852 1. The product is in product factory default state.
 1853 2. Documentation describing the credential provisioning approach is available.

1854 **Assessment activities**

- 1855 1. Review documentation to identify the credential provisioning approach during secure production.
 1856 2. Inspect factory default credentials across at least two product units. Verify that credentials differ across units.
 1857 3. Attempt to operate the product with shared default credentials.

1858 **Assessment verdict**

1859 The verdict fail is assigned if any of the following conditions apply:

- 1860 1. Documentation does not describe the credential provisioning approach during secure production.
 1861 2. The product does not provide unique credentials across product units.
 1862 3. The product operates with shared default credentials.

1863 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1864 1. Documentation describes the credential provisioning approach during secure production.
 1865 2. The product provides unique credentials across product units.
 1866 3. The product does not operate with shared default credentials.

1867 **Assessment evidence**

- 1868 1. Documentation describing the credential provisioning approach during secure production.
 1869 2. Test results showing the product provides unique credentials across product units.
 1870 3. Test results showing shared default credentials do not provide access.
 1871

1872 [\[AC-AUTH-1-03\]](#) Verify that where the product transmits critical security parameters, the product protects their
 1873 transmission over a secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

1874 **Assessment reference**

1875 Requirement [\[RQ-AUTH-1-03\]](#).

1876 **Assessment objective**

1877 Confirm that where the product transmits critical security parameters, the product protects their transmission over a
 1878 secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

1879 **Assessment preparation**

- 1880 1. The product is in product operational state.
 1881 2. Documentation describing the critical security parameter transmission mechanism and secure channel is
 1882 available.

1883 **Assessment activities**

- 1884 1. Review documentation to identify the secure channel used for critical security parameter transmission.
 1885 2. Capture network traffic during an authentication attempt on each interface that accepts critical security
 1886 parameters. Verify the product transmits critical security parameters over a secure channel.
 1887 3. Attempt to force critical security parameter transmission over an unencrypted channel. Verify that the product
 1888 prevents disclosure of critical security parameters.

1889 **Assessment verdict**

1890 The verdict fail is assigned if any of the following conditions apply:

- 1891 1. Documentation does not describe the secure channel used for critical security parameter transmission.
 1892 2. The product does not protect critical security parameters over a secure channel on any interface.
 1893 3. The product does not prevent disclosure of critical security parameters over an unencrypted channel.

1894 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1895 1. Documentation describes the secure channel used for critical security parameter transmission.
 1896 2. The product protects critical security parameters over a secure channel on all interfaces.
 1897 3. The product prevents disclosure of critical security parameters over an unencrypted channel.

1898 **Assessment evidence**

- 1899 1. Documentation describing the secure channel used for critical security parameter transmission.
 1900 2. Test results showing the product protects critical security parameters over a secure channel when transmitting
 1901 on all interfaces.
 1902 3. Test results showing the product prevents disclosure of critical security parameters when an unencrypted
 1903 channel is forced.
 1904

1905 [\[AC-AUTH-1-04\]](#) Verify that the product protects critical security parameters using state of the art cryptography.

1906 **Assessment reference**

1907 Requirement [\[RQ-AUTH-1-04\]](#).

1908 **Assessment objective**

1909 Confirm that the product protects critical security parameters using state of the art cryptography.

1910 **Assessment preparation**

- 1911 1. The product is in product operational state with at least one user account configured.
 1912 2. Documentation describing the critical security parameter storage mechanism is available.

1913 **Assessment activities**

- 1914 1. Review documentation to identify the cryptographic method used for critical security parameter storage and its
 1915 parameters. Verify the documented method is state of the art.

- 1916 2. Inspect stored critical security parameters where storage is accessible, verifying they are not in plaintext and
 1917 that a known-credential stored representation is consistent with the documented method. Inspect manufacturer
 1918 technical documentation or source code where direct storage access is not available to confirm the
 1919 implementation matches the documented method.
- 1920 3. Attempt to retrieve critical security parameters in plaintext through available interfaces without required
 1921 authorization. Verify the product protects critical security parameters by denying retrieval.

1922 **Assessment verdict**

1923 The verdict fail is assigned if any of the following conditions apply:

- 1924 1. Documentation does not describe the critical security parameter storage method.
 1925 2. The product does not use a state of the art critical security parameter storage method.
 1926 3. The product stores critical security parameters in plaintext.
 1927 4. The product does not store critical security parameters consistently with the documented method.
 1928 5. The product permits retrieval of critical security parameters in plaintext without authorization.

1929 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1930 1. Documentation describes the critical security parameter storage method.
 1931 2. The product uses a state of the art critical security parameter storage method.
 1932 3. The product does not store critical security parameters in plaintext.
 1933 4. The product stores critical security parameters consistently with the documented method.
 1934 5. The product does not permit retrieval of critical security parameters in plaintext without authorization.

1935 **Assessment evidence**

- 1936 1. Documentation describing the critical security parameter storage method, parameters, and standard reference.
 1937 2. Test results showing the storage method is state of the art.
 1938 3. Test results showing critical security parameters are not stored in plaintext, where direct access is available.
 1939 4. Test results showing stored representation matches the documented method.
 1940 5. Test results showing the implementation matches the documented storage method, where direct storage access
 1941 is not available.
 1942 6. Test results showing critical security parameters cannot be retrieved in plaintext without authorization.
 1943

1944 [\[AC-AUTH-1-05\]](#) Verify that the product enforces minimum credential entropy requirements.

1945 **Assessment reference**

1946 Requirement [\[RQ-AUTH-1-05\]](#).

1947 **Assessment objective**

1948 Confirm that the product enforces minimum credential entropy requirements, and that the product rejects credentials
 1949 that do not meet the minimum entropy.

1950 **Assessment preparation**

- 1951 1. The product is in product operational state.
 1952 2. Documentation describing minimum credential entropy requirements is available.

1953 **Assessment activities**

- 1954 1. Review documentation to identify the minimum credential entropy requirements.
 1955 2. Attempt to create or change a credential that does not meet the documented minimum entropy. Verify the
 1956 product rejects the credential.
 1957 3. Create or change a credential that meets the minimum entropy. Verify the product accepts it.

1958 **Assessment verdict**

1959 The verdict fail is assigned if any of the following conditions apply:

- 1960 1. Documentation does not describe the minimum credential entropy requirements.
 1961 2. The product does not reject credentials that do not meet the minimum entropy.
 1962 3. The product does not accept credentials meeting the minimum entropy.

1963 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 1964 1. Documentation describes the minimum credential entropy requirements.
 1965 2. The product rejects credentials that do not meet the minimum entropy.
 1966 3. The product accepts credentials meeting the minimum entropy.

1967 **Assessment evidence**

- 1968 1. Documentation describing the minimum credential entropy requirements.
 1969 2. Test results showing credentials that do not meet the minimum entropy are rejected.
 1970 3. Test results showing credentials meeting the minimum entropy are accepted.
 1971

1972 [\[AC-AUTH-1-06\]](#) Verify that the product enforces authentication failure protection by (i) progressive delays between
 1973 failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

1974 **Assessment reference**

1975 Requirement [\[RO-AUTH-1-06\]](#).

1976 **Assessment objective**

1977 Confirm that the product enforces authentication failure protection by (i) progressive delays between failed attempts;
 1978 and (ii) temporary account lockout after a configurable number of failed attempts, and that both mechanisms are
 1979 documented with specific thresholds and durations.

1980 **Assessment preparation**

- 1981 1. The product is in product operational state with at least one user account.
 1982 2. Documentation describing the authentication failure protection mechanisms is available.

1983 **Assessment activities**

- 1984 1. Review documentation to identify the authentication failure protection parameters.
 1985 2. Perform consecutive failed authentication attempts using invalid credentials and measure the delay between
 1986 allowed attempts. Verify the delay increases progressively with consecutive failures.
 1987 3. Reset the authentication failure counter by successfully authenticating, then perform consecutive failed
 1988 attempts from a clean zero-failure state until the documented lockout threshold is reached. Verify the account
 1989 is temporarily locked and the lockout duration matches the documented value.
 1990 4. Wait for lockout to expire and authenticate with valid credentials. Verify access is granted and failure counters
 1991 are reset.

1992 **Assessment verdict**

1993 The verdict fail is assigned if any of the following conditions apply:

- 1994 1. Documentation does not describe authentication failure protection mechanisms.
 1995 2. Documentation does not list lockout threshold and duration values.
 1996 3. The product does not apply a delay between consecutive failed authentication attempts.
 1997 4. The product does not increase the delay with each consecutive failure.
 1998 5. The product does not lock the account after consecutive failed authentication attempts reach the documented
 1999 lockout threshold.
 2000 6. The product does not enforce the documented lockout duration.
 2001 7. The product does not restore access with valid credentials after lockout expires.
 2002 8. The product does not reset the failure counter after successful authentication following lockout.

2003 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2004 1. Documentation describes authentication failure protection mechanisms.
 2005 2. Documentation lists lockout threshold and duration values.
 2006 3. The product applies a delay between consecutive failed authentication attempts.
 2007 4. The product increases the delay with each consecutive failure.
 2008 5. The product locks the account after consecutive failed authentication attempts reach the documented lockout
 2009 threshold.
 2010 6. The product enforces the documented lockout duration.

- 2011 7. The product restores access with valid credentials after lockout expires.
 2012 8. The product resets the failure counter after successful authentication following lockout.

2013 **Assessment evidence**

- 2014 1. Documentation describing authentication failure protection mechanisms.
 2015 2. Documentation listing lockout threshold and duration values.
 2016 3. Test results showing the product applies progressive delays between consecutive failed authentication
 2017 attempts.
 2018 4. Test results showing the delay increases with each consecutive failure.
 2019 5. Test results from resetting the failure counter and performing consecutive failed authentication attempts
 2020 showing the product locks the account after the documented lockout threshold is reached.
 2021 6. Test results showing the product enforces the documented lockout duration.
 2022 7. Test results showing the product restores access with valid credentials after lockout expires.
 2023 8. Test results showing the product resets the failure counter after successful authentication following lockout.
 2024

2025 [\[AC-AUTH-1-07\]](#) Verify that the product stores previously used passwords using state of the art cryptography,
 2026 validates password changes against this history before acceptance, and stores at least the minimum number of previous
 2027 passwords as given in [TBL-password-history-depth].

2028 **Assessment reference**

2029 Requirement [\[RQ-AUTH-1-07\]](#).

2030 **Assessment objective**

2031 Confirm that the product stores previously used passwords using state of the art cryptography, validates password
 2032 changes against this history, and meets the graduated minimum number of stored passwords.

2033 **Assessment preparation**

- 2034 1. The product is in product operational state with at least one user account.
 2035 2. Documentation describing the password history mechanism is available.

2036 **Assessment activities**

- 2037 1. Review documentation to identify which management risk factors apply to the product. Verify the applicable
 2038 minimum number of previous passwords from [TBL-password-history-depth].
 2039 2. Review documentation to identify the password history depth and the cryptographic method used for storage.
 2040 3. Verify the documented password history depth meets the graduated minimum for the applicable risk factors.
 2041 4. Use the password change interface to (i) set a known password; (ii) change it to a different value; and (iii)
 2042 attempt to change it back to the original value. Verify the product rejects the change and informs the user that
 2043 the password is already present in the password history.
 2044 5. Change the password to a value that is not present in the password history. Verify the change is accepted.
 2045 6. Inspect the password history where storage is accessible. Verify previous passwords are stored using state of
 2046 the art cryptography, not in plaintext.
 2047 7. Test password history isolation across accounts by (i) configuring two separate user accounts; (ii) changing the
 2048 password on one account; and (iii) attempting to reuse that same password on the other account. Verify the
 2049 history of one account does not affect password validation on the other.

2050 **Assessment verdict**

2051 The verdict fail is assigned if any of the following conditions apply:

- 2052 1. Documentation does not list which risk factors apply to the product.
 2053 2. Documentation does not describe the password history mechanism or cryptographic storage method.
 2054 3. The product does not store the graduated minimum number of previous passwords for the applicable risk level.
 2055 4. The product does not reject password changes to passwords present in the history.
 2056 5. The product does not inform the user of the rejection reason.
 2057 6. The product does not accept new passwords not present in the history.
 2058 7. The product does not store password history using state of the art cryptography.
 2059 8. The product does not isolate password history across accounts.

- 2060 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2061 1. Documentation lists which risk factors apply to the product.
 - 2062 2. Documentation describes the password history mechanism and cryptographic storage method.
 - 2063 3. The product stores the graduated minimum number of previous passwords for the applicable risk level.
 - 2064 4. The product rejects password changes to passwords present in the history.
 - 2065 5. The product informs the user of the rejection reason.
 - 2066 6. The product accepts new passwords not present in the history.
 - 2067 7. The product stores password history using state of the art cryptography.
 - 2068 8. The product isolates password history across accounts.

2069 **Assessment evidence**

- 2070 1. Documentation listing which risk factors apply to the product.
- 2071 2. Documentation describing the password history mechanism, depth, and cryptographic storage method.
- 2072 3. Test results showing the product stores the graduated minimum number of previous passwords for the applicable risk level.
- 2073 4. Test results showing passwords present in the password history are rejected.
- 2074 5. Test results showing the user is informed of the rejection reason.
- 2075 6. Test results showing new passwords not present in history are accepted.
- 2076 7. Test results showing the product stores password history using state of the art cryptography.
- 2077 8. Test results showing the product isolates password history across accounts.

2079

2080 **6.5.2 [AUTH-2] Authorization**

2081 **6.5.2.1 Requirement assessments**

2082 [\[AC-AUTH-2-01\]](#) Verify that where the product supports more than one privilege level, the product enforces privilege
2083 separation.

2084 **Assessment reference**

2085 Requirement [\[RO-AUTH-2-01\]](#).

2086 **Assessment objective**

2087 Confirm that where the product supports more than one privilege level, the product enforces privilege separation.

2088 **Assessment preparation**

- 2089 1. The product is in product operational state.
- 2090 2. Documentation describing the privilege levels is available, where the product supports more than one privilege
2091 level.

2092 **Assessment activities**

- 2093 1. Review documentation to identify whether the product supports more than one privilege level. Verify that the
2094 documentation describes all privilege levels and the authentication mechanism for management access, where
2095 applicable.
- 2096 2. Attempt to access management functions without authentication, where the product supports more than one
2097 privilege level. Verify access is denied.
- 2098 3. Authenticate with non-management credentials and attempt to access management functions, where the
2099 product supports more than one privilege level. Verify access is denied.
- 2100 4. Authenticate with management credentials, where the product supports more than one privilege level. Verify
2101 management functions are accessible.

2102 **Assessment verdict**

2103 The verdict fail is assigned if any of the following conditions apply:

- 2104 1. Documentation does not describe all supported privilege levels or the authentication mechanism for
2105 management access.
- 2106 2. The product does not deny access without authentication to management functions.

- 2107 3. The product grants management access with non-management credentials.
- 2108 4. The product does not grant access to management functions with management credentials.
- 2109 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2110 1. Documentation describes all supported privilege levels and the authentication mechanism for management
- 2111 access.
- 2112 2. The product denies access without authentication to management functions.
- 2113 3. The product does not grant management access with non-management credentials.
- 2114 4. The product grants access to management functions with management credentials.
- 2115 **Assessment evidence**
- 2116 1. Documentation describing all supported privilege levels and the authentication mechanism for management
- 2117 access.
- 2118 2. Test results showing management access attempts without authentication are denied.
- 2119 3. Test results showing non-management credentials cannot access management functions.
- 2120 4. Test results showing management credentials grant access to management functions.
- 2121
- 2122 [\[AC-AUTH-2-02\]](#) Verify that the product restricts each user to their authorized privilege level.
- 2123 **Assessment reference**
- 2124 Requirement [\[RQ-AUTH-2-02\]](#).
- 2125 **Assessment objective**
- 2126 Confirm that the product restricts each user to their authorized privilege level.
- 2127 **Assessment preparation**
- 2128 1. The product is in product operational state.
- 2129 2. Documentation describing all privilege levels and the operations assigned to each level is available.
- 2130 **Assessment activities**
- 2131 1. Review documentation to identify all privilege levels and the operations assigned to each.
- 2132 2. Authenticate with an account at each privilege level and attempt all documented operations for that level.
- 2133 Verify they succeed.
- 2134 3. Authenticate with an account at each defined privilege level in turn and attempt operations assigned to a higher
- 2135 privilege level. Verify each attempt is denied.
- 2136 **Assessment verdict**
- 2137 The verdict fail is assigned if any of the following conditions apply:
- 2138 1. Documentation does not describe all privilege levels.
- 2139 2. Documentation does not describe the operations assigned to each privilege level.
- 2140 3. The product does not permit each user to perform all operations within their assigned privilege level.
- 2141 4. The product does not restrict users from performing operations above their assigned privilege level.
- 2142 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2143 1. Documentation describes all privilege levels.
- 2144 2. Documentation describes the operations assigned to each privilege level.
- 2145 3. The product permits each user to perform all operations within their assigned privilege level.
- 2146 4. The product restricts users from performing operations above their assigned privilege level.
- 2147 **Assessment evidence**
- 2148 1. Documentation describing all privilege levels.
- 2149 2. Documentation describing the operations assigned to each privilege level.
- 2150 3. Test results showing the product permits each user to perform all operations within their assigned privilege
- 2151 level.
- 2152 4. Test results showing the product restricts users from performing operations above their assigned privilege
- 2153 level.

2154

2155 [\[AC-AUTH-2-03\]](#) Verify that the product enforces access control on all interfaces providing access to the product.2156 **Assessment reference**2157 Requirement [\[RO-AUTH-2-03\]](#).2158 **Assessment objective**

2159 Confirm that the product enforces access control on all interfaces providing access to the product.

2160 **Assessment preparation**

2161 1. The product is in product operational state.

2162 2. Documentation listing all interfaces providing access to the product and the access control mechanisms on
2163 each is available.2164 **Assessment activities**2165 1. Review documentation to identify all interfaces providing access to the product and the access control
2166 mechanism on each.2167 2. Attempt access on each interface providing access to the product. Verify that the product enforces access
2168 control on each interface.2169 **Assessment verdict**

2170 The verdict fail is assigned if any of the following conditions apply:

2171 1. Documentation does not describe all interfaces providing access to the product and their access control
2172 mechanisms.

2173 2. The product does not enforce access control on any interface providing access to the product.

2174 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

2175 1. Documentation describes all interfaces providing access to the product and their access control mechanisms.

2176 2. The product enforces access control on each interface providing access to the product.

2177 **Assessment evidence**2178 1. Documentation describing all interfaces providing access to the product and the access control mechanism for
2179 each.2180 2. Test results showing the product enforces access control on each interface providing access to the product.
21812182 [\[AC-AUTH-2-04\]](#) Verify that the product validates each command based on the authorized privilege level before
2183 execution.2184 **Assessment reference**2185 Requirement [\[RO-AUTH-2-04\]](#).2186 **Assessment objective**

2187 Confirm that the product validates each command based on the authorized privilege level before execution.

2188 **Assessment preparation**

2189 1. The product is in product operational state.

2190 2. Documentation describing the command authorization mechanism is available.

2191 **Assessment activities**2192 1. Review documentation to identify the command authorization mechanism and the privilege level required for
2193 each command category.2194 2. Authenticate with a lower-privilege account and attempt to execute commands from each higher-privilege
2195 category. Verify each is denied before execution.2196 3. Authenticate with an authorized account and execute commands from the authorized category. Verify they
2197 succeed.

- 2198 4. Attempt to bypass command authorization by modifying command parameters or injecting commands through
2199 alternative input paths. Verify the product denies execution.

2200 **Assessment verdict**

2201 The verdict fail is assigned if any of the following conditions apply:

- 2202 1. Documentation does not describe the command authorization mechanism or privilege requirements per
2203 command category.
- 2204 2. The product does not validate privilege levels before command execution.
- 2205 3. The product does not reject higher-privilege commands from lower-privilege users.
- 2206 4. The product does not execute authorized commands successfully.
- 2207 5. The product does not deny execution when command parameters are modified or commands are injected
2208 through alternative input paths.

2209 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2210 1. Documentation describes the command authorization mechanism and privilege requirements per command
2211 category.
- 2212 2. The product validates privilege levels before command execution.
- 2213 3. The product rejects higher-privilege commands from lower-privilege users.
- 2214 4. The product executes authorized commands successfully.
- 2215 5. The product denies execution when command parameters are modified or commands are injected through
2216 alternative input paths.

2217 **Assessment evidence**

- 2218 1. Documentation describing the command authorization mechanism and privilege requirements per command
2219 category.
- 2220 2. Test results showing the product validates privilege levels before command execution.
- 2221 3. Test results showing the product rejects higher-privilege commands from lower-privilege users.
- 2222 4. Test results showing authorized commands execute successfully for authorized accounts.
- 2223 5. Test results showing the product denies execution when command parameters are modified or commands are
2224 injected through alternative input paths.
- 2225

2226 **6.5.3 [AUTH-3] Authenticated session lifecycle**

2227 **6.5.3.1 Requirement assessments**

2228 [\[AC-AUTH-3-01\]](#) Verify that the product generates session identifiers that are unique, non-predictable, and resistant to
2229 brute force attacks, using state of the art cryptography.

2230 **Assessment reference**

2231 Requirement [\[RQ-AUTH-3-01\]](#).

2232 **Assessment objective**

2233 Confirm that the product generates session identifiers that are unique, non-predictable, and resistant to brute force
2234 attacks, using state of the art cryptography.

2235 **Assessment preparation**

- 2236 1. The product is in product operational state with at least one authenticated session-capable interface.
- 2237 2. Documentation describing the session identifier generation mechanism is available.

2238 **Assessment activities**

- 2239 1. Review documentation to identify the session identifier generation mechanism. Verify the documented session
2240 identifier generation mechanism is state of the art.
- 2241 2. Establish at least 10 concurrent sessions. Verify that each session identifier is distinct.
- 2242 3. Test session identifier invalidation by (i) establishing an authenticated session and recording the identifier; (ii)
2243 invalidating the session; and (iii) immediately attempting to reuse the recorded identifier. Verify the product
2244 rejects the reused identifier.

2245 4. Attempt to authenticate using a fabricated session identifier. Verify the product rejects it.

2246 **Assessment verdict**

2247 The verdict fail is assigned if any of the following conditions apply:

- 2248 1. Documentation does not describe the session identifier generation mechanism.
- 2249 2. The product does not use a state of the art session identifier generation mechanism.
- 2250 3. Any concurrent session identifier is not distinct.
- 2251 4. The product does not reject a reused session identifier immediately after invalidation of an authenticated session.
- 2252 2252
- 2253 5. The product does not reject fabricated session identifiers.

2254 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2255 1. Documentation describes the session identifier generation mechanism.
- 2256 2. The product uses a state of the art session identifier generation mechanism.
- 2257 3. All concurrent session identifiers are distinct.
- 2258 4. The product rejects a reused session identifier immediately after invalidation of an authenticated session.
- 2259 5. The product rejects fabricated session identifiers.

2260 **Assessment evidence**

- 2261 1. Documentation describing the session identifier generation mechanism.
- 2262 2. Test results showing the session identifier generation mechanism is state of the art.
- 2263 3. Test results showing all concurrent session identifiers are distinct.
- 2264 4. Test results showing the product rejects a reused session identifier immediately after invalidation of an authenticated session.
- 2265 2265
- 2266 5. Test results showing fabricated session identifiers are rejected.
- 2267

2268 [\[AC-AUTH-3-02\]](#) Verify that the product enforces session timeout with configurable idle timeout periods and default values.
2269

2270 **Assessment reference**

2271 Requirement [\[RQ-AUTH-3-02\]](#).

2272 **Assessment objective**

2273 Confirm that the product enforces session timeout with configurable idle timeout periods and default values.

2274 **Assessment preparation**

- 2275 1. The product is in product operational state with at least one authenticated session.
- 2276 2. Documentation describing session timeout mechanisms, default timeout values, and configuration options is available.
- 2277

2278 **Assessment activities**

- 2279 1. Review documentation to identify the default idle timeout value and the configurable range.
- 2280 2. Retrieve the default idle timeout value from documentation or product configuration and leave an authenticated session idle for that timeout period. Verify that the product terminates the session and requires re-authentication.
- 2281 2281
- 2282 2282
- 2283 3. Establish a new session and perform an operation during the timeout period. Verify the timeout counter resets and the session remains active.
- 2284 2284
- 2285 4. Configure the timeout period to a shorter value. Verify that the session terminates after the new period.
- 2286 5. Attempt to reuse a timed-out session. Verify that the product denies access.

2287 **Assessment verdict**

2288 The verdict fail is assigned if any of the following conditions apply:

- 2289 1. Documentation does not describe the default idle timeout value and configurable range.
- 2290 2. The product does not terminate sessions after the default idle timeout period.
- 2291 3. The product does not require re-authentication after session termination by idle timeout.

- 2292 4. The product does not reset the timeout counter when user activity occurs, or the session does not remain active.
 2293 5. The product does not enforce configurable timeout periods.
 2294 6. The product does not apply newly configured timeout values.
 2295 7. The product does not deny access when a timed-out session is reused.

2296 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2297 1. Documentation describes the default idle timeout value and configurable range.
 2298 2. The product terminates sessions after the default idle timeout period.
 2299 3. The product requires re-authentication after session termination by idle timeout.
 2300 4. The product resets the timeout counter when user activity occurs and the session remains active.
 2301 5. The product enforces configurable timeout periods.
 2302 6. The product applies newly configured timeout values.
 2303 7. The product denies access when a timed-out session is reused.

2304 **Assessment evidence**

- 2305 1. Documentation describing the session timeout mechanism, default idle timeout value, and configurable range.
 2306 2. Test results showing the product terminates sessions after the default idle timeout period.
 2307 3. Test results showing the product requires re-authentication after session termination by idle timeout.
 2308 4. Test results showing the timeout counter resets on user activity and the session remains active.
 2309 5. Test results showing the product enforces configurable timeout periods.
 2310 6. Test results showing the product applies newly configured timeout values.
 2311 7. Test results showing access is denied when a timed-out session is reused.
 2312

2313 [\[AC-AUTH-3-03\]](#) Verify that the product invalidates sessions immediately upon (i) session logout or termination; (ii)
 2314 authentication credential change; or (iii) timeout expiration.

2315 **Assessment reference**

2316 Requirement [\[RO-AUTH-3-03\]](#).

2317 **Assessment objective**

2318 Confirm that the product invalidates sessions immediately upon (i) session logout or termination; (ii) authentication
 2319 credential change; or (iii) timeout expiration, and that invalidated sessions cannot be reused.

2320 **Assessment preparation**

- 2321 1. The product is in product operational state with at least one authenticated session.
 2322 2. Documentation describing session invalidation triggers and data removal mechanisms is available.

2323 **Assessment activities**

- 2324 1. Review documentation to identify all session invalidation triggers and data removal mechanisms.
 2325 2. Establish an authenticated session and perform a logout. Establish a second session and terminate it through
 2326 the management interface. Verify that the product denies access when either session identifier is reused.
 2327 3. Establish a session and change the authentication credential for the account. Verify that the product invalidates
 2328 the existing session and requires re-authentication.
 2329 4. Allow an established session to time out. Verify that the product denies access when the session identifier is
 2330 reused.
 2331 5. Trigger each session invalidation type in sequence and time each invalidation from trigger event to denial of
 2332 the session identifier. Verify no observable delay occurs.

2333 **Assessment verdict**

2334 The verdict fail is assigned if any of the following conditions apply:

- 2335 1. Documentation does not describe all invalidation triggers and data removal mechanisms.
 2336 2. The product does not invalidate sessions upon logout or termination.
 2337 3. The product does not reject invalidated session identifiers on subsequent use.
 2338 4. The product does not invalidate sessions upon authentication credential change.
 2339 5. The product does not invalidate sessions upon timeout expiration.

- 2340 6. The product does not invalidate sessions without observable delay for all triggers.
- 2341 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 2342 1. Documentation describes all invalidation triggers and data removal mechanisms.
- 2343 2. The product invalidates sessions upon logout or termination.
- 2344 3. The product rejects invalidated session identifiers on subsequent use.
- 2345 4. The product invalidates sessions upon authentication credential change.
- 2346 5. The product invalidates sessions upon timeout expiration.
- 2347 6. The product invalidates sessions without observable delay for all triggers.

2348 **Assessment evidence**

- 2349 1. Documentation describing all session invalidation triggers and data removal mechanisms.
- 2350 2. Test results showing the product invalidates sessions upon logout or termination.
- 2351 3. Test results showing the product rejects invalidated session identifiers on subsequent use.
- 2352 4. Test results showing the product invalidates sessions upon authentication credential change.
- 2353 5. Test results showing the product invalidates sessions upon timeout expiration.
- 2354 6. Test results showing the product invalidates sessions without observable delay for all triggers.
- 2355

2356 [\[AC-AUTH-3-04\]](#) Verify that the product restricts session identifiers to the session management mechanism.

2357 **Assessment reference**

2358 Requirement [\[RQ-AUTH-3-04\]](#).

2359 **Assessment objective**

2360 Confirm that the product restricts session identifiers to the session management mechanism.

2361 **Assessment preparation**

- 2362 1. The product is in product operational state with at least one authenticated session.
- 2363 2. Documentation describing session identifier protection mechanisms and the secure channel used is available.

2364 **Assessment activities**

- 2365 1. Review documentation to identify the secure channel protocol and the session token protection mechanism for each interface type.
- 2366
- 2367 2. Capture network traffic during session establishment and use. Verify the captured traffic uses state of the art cryptography.
- 2368
- 2369 3. Verify that the product implements session token protection mechanisms for each interface type.
- 2370 4. Inspect audit events generated during session activity. Verify session identifiers do not appear in audit events.
- 2371 5. Attempt to force session identifier transmission over an unencrypted channel. Verify the product does not transmit the session identifier.
- 2372

2373 **Assessment verdict**

2374 The verdict fail is assigned if any of the following conditions apply:

- 2375 1. Documentation does not describe the secure channel protocol and token protection mechanism for any interface type.
- 2376
- 2377 2. The product does not transmit session identifiers using state of the art cryptography.
- 2378 3. The product does not implement session token protection mechanisms for any interface type.
- 2379 4. The product discloses session identifiers in audit events.
- 2380 5. The product transmits session identifiers over unencrypted channels.

2381 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2382 1. Documentation describes the secure channel protocol and token protection mechanism for each interface type.
- 2383 2. The product transmits session identifiers using state of the art cryptography.
- 2384 3. The product implements session token protection mechanisms for each interface type.
- 2385 4. The product does not disclose session identifiers in audit events.
- 2386 5. The product does not transmit session identifiers over unencrypted channels.

2387 **Assessment evidence**

- 2388 1. Documentation describing session identifier protection mechanisms and the secure channel for each interface
- 2389 type.
- 2390 2. Test results from network traffic captures during session establishment show state of the art cryptography.
- 2391 3. Test results showing session token protection mechanisms are implemented for each interface type.
- 2392 4. Test results showing session identifiers do not appear in audit events.
- 2393 5. Test results showing the product does not transmit session identifiers over unencrypted channels.
- 2394

2395 [\[AC-AUTH-3-05\]](#) Verify that the product limits concurrent sessions to a configurable maximum per user account.

2396 **Assessment reference**

2397 Requirement [\[RQ-AUTH-3-05\]](#).

2398 **Assessment objective**

2399 Confirm that the product limits concurrent sessions to a configurable maximum per user account.

2400 **Assessment preparation**

- 2401 1. The product is in product operational state.
- 2402 2. Documentation describing the concurrent session limit mechanism is available.

2403 **Assessment activities**

- 2404 1. Review documentation to identify the default concurrent session limit and the configurable range.
- 2405 2. Establish sessions up to the documented limit. Verify that all are active.
- 2406 3. Attempt to establish one session beyond the limit. Verify that the product denies the additional session.
- 2407 4. Change the concurrent session limit to a different value. Verify the new limit is enforced.
- 2408 5. Verify the limit is enforced per user account.

2409 **Assessment verdict**

2410 The verdict fail is assigned if any of the following conditions apply:

- 2411 1. Documentation does not describe the default concurrent session limit, configurable range, and behaviour when
- 2412 the limit is exceeded.
- 2413 2. The product does not accept sessions up to the documented concurrent session limit.
- 2414 3. The product does not deny session establishment beyond the configured concurrent session limit.
- 2415 4. The product does not enforce the newly configured concurrent session limit.
- 2416 5. The product does not enforce the concurrent session limit independently per user account.

2417 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2418 1. Documentation describes the default concurrent session limit, configurable range, and behaviour when the
- 2419 limit is exceeded.
- 2420 2. The product accepts sessions up to the documented concurrent session limit.
- 2421 3. The product denies session establishment beyond the configured concurrent session limit.
- 2422 4. The product enforces the newly configured concurrent session limit.
- 2423 5. The product enforces the concurrent session limit independently per user account.

2424 **Assessment evidence**

- 2425 1. Documentation describing the concurrent session limit, configurable range, and behaviour when the limit is
- 2426 exceeded.
- 2427 2. Test results showing sessions up to the documented limit are active.
- 2428 3. Test results showing the product denies session establishment beyond the configured concurrent session limit.
- 2429 4. Test results showing the product enforces the newly configured concurrent session limit.
- 2430 5. Test results showing the concurrent session limit applies independently to each user account.
- 2431

2432 [\[AC-AUTH-3-06\]](#) Verify that the product denies privilege escalation attempts without authorization within active

2433 sessions.

2434 **Assessment reference**2435 Requirement [\[RQ-AUTH-3-06\]](#).2436 **Assessment objective**

2437 Confirm that the product denies privilege escalation attempts without authorization within active sessions.

2438 **Assessment preparation**

- 2439 1. The product is in product operational state with at least one non-management authenticated session.
- 2440 2. Documentation describing the privilege escalation denial mechanism is available.

2441 **Assessment activities**

- 2442 1. Review documentation to identify the privilege escalation denial mechanism.
- 2443 2. Attempt privilege escalation from a non-management session through (i) parameter manipulation; and (ii)
- 2444 session attribute tampering. Verify the product denies each attempt.

2445 **Assessment verdict**

2446 The verdict fail is assigned if any of the following conditions apply:

- 2447 1. Documentation does not describe the privilege escalation denial mechanism.
- 2448 2. The product does not deny privilege escalation attempts without authorization from non-management sessions.

2449 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2450 1. Documentation describes the privilege escalation denial mechanism.
- 2451 2. The product denies privilege escalation attempts without authorization from non-management sessions.

2452 **Assessment evidence**

- 2453 1. Documentation describing the privilege escalation denial mechanism.
- 2454 2. Test results showing the product denies privilege escalation attempts without authorization from non-
- 2455 management sessions.

2456

2457 **6.5.4 [AUTH-4] Protocol access control**2458 **6.5.4.1 Requirement assessments**

2459 [\[AC-AUTH-4-01\]](#) Verify that the product enables only management protocols using state of the art cryptography in
 2460 product factory default state and in product operational state.

2461 **Assessment reference**2462 Requirement [\[RQ-AUTH-4-01\]](#).2463 **Assessment objective**

2464 Confirm that the product enables only management protocols using state of the art cryptography in product factory
 2465 default state and in product operational state.

2466 **Assessment preparation**

- 2467 1. The product is in product factory default state.
- 2468 2. Documentation describing management protocols is available.

2469 **Assessment activities**

- 2470 1. Review documentation to identify all management protocols and their cryptographic protection.
- 2471 2. Inspect the product in product factory default state to enumerate all enabled management protocols. Verify
- 2472 each uses state of the art cryptography.
- 2473 3. Complete product initialization and inspect the product in product operational state to enumerate all enabled
- 2474 management protocols. Verify each uses state of the art cryptography.
- 2475 4. Capture network traffic during a management session on each enabled protocol in product operational state.
- 2476 Verify the captured traffic uses state of the art cryptography.

- 2477 5. Attempt to enable a management protocol that does not use state of the art cryptography. Verify that the
2478 product denies the protocol activation or informs the user.

2479 **Assessment verdict**

2480 The verdict fail is assigned if any of the following conditions apply:

- 2481 1. Documentation does not list all management protocols or their cryptographic protection.
- 2482 2. Any management protocol enabled in product factory default state does not use state of the art cryptography.
- 2483 3. Any management protocol enabled in product operational state does not use state of the art cryptography.
- 2484 4. Any enabled management protocol does not use state of the art cryptography in product operational state.
- 2485 5. The product does not deny activation of protocols terminated by the product that do not use state of the art
2486 cryptography.

2487 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2488 1. Documentation lists all management protocols and their cryptographic protection.
- 2489 2. All management protocols enabled in product factory default state use state of the art cryptography.
- 2490 3. All management protocols enabled in product operational state use state of the art cryptography.
- 2491 4. All enabled management protocols use state of the art cryptography in product operational state.
- 2492 5. The product denies activation of protocols terminated by the product that do not use state of the art
2493 cryptography.

2494 **Assessment evidence**

- 2495 1. Documentation listing all management protocols and their cryptographic protection.
- 2496 2. Test results showing all management protocols enabled in product factory default state use state of the art
2497 cryptography.
- 2498 3. Test results showing all management protocols enabled in product operational state use state of the art
2499 cryptography.
- 2500 4. Test results from network traffic captures confirming all enabled management protocols use state of the art
2501 cryptography in product operational state.
- 2502 5. Test results showing the product denies activation of protocols terminated by the product that do not use state
2503 of the art cryptography.

2504

2505 [\[AC-AUTH-4-02\]](#) Verify that the product enforces rate limiting for each protocol that accepts requests without
2506 authentication.

2507 **Assessment reference**

2508 Requirement [\[RQ-AUTH-4-02\]](#).

2509 **Assessment objective**

2510 Confirm that the product enforces rate limiting for each protocol that accepts requests without authentication.

2511 **Assessment preparation**

- 2512 1. The product is in product operational state.
- 2513 2. Documentation describing the rate limiting mechanism is available.

2514 **Assessment activities**

- 2515 1. Review documentation to identify the rate limiting thresholds for each protocol that accepts requests without
2516 authentication.
- 2517 2. Exceed the documented rate limiting threshold on each protocol that accepts requests without authentication.
2518 Verify the product drops requests after the threshold is reached.
- 2519 3. Send requests without authentication below the documented rate limiting threshold on each protocol. Verify
2520 the product does not block them.

2521 **Assessment verdict**

2522 The verdict fail is assigned if any of the following conditions apply:

- 2523 1. Documentation does not list rate limiting thresholds for any protocol that accepts requests without
2524 authentication.

- 2525 2. The product does not drop requests that exceed the documented rate limiting threshold.
 2526 3. The product blocks requests below the documented rate limiting threshold.

2527 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2528 1. Documentation lists rate limiting thresholds for each protocol that accepts requests without authentication.
 2529 2. The product drops requests that exceed the documented rate limiting threshold.
 2530 3. The product does not block requests below the documented rate limiting threshold.

2531 **Assessment evidence**

- 2532 1. Documentation listing rate limiting thresholds for each protocol that accepts requests without authentication.
 2533 2. Test results showing the product enforces rate limiting by dropping requests exceeding the documented
 2534 threshold.
 2535 3. Test results showing requests below the documented rate limiting threshold are not blocked.
 2536

2537 [\[AC-AUTH-4-03\]](#) Verify that the product provides capability to configure state of the art cryptography and to disable
 2538 protocols that do not use state of the art cryptography.

2539 **Assessment reference**

2540 Requirement [\[RQ-AUTH-4-03\]](#).

2541 **Assessment objective**

2542 Confirm that the product provides capability to configure state of the art cryptography and to disable protocols that do
 2543 not use state of the art cryptography.

2544 **Assessment preparation**

- 2545 1. The product is in product operational state.
 2546 2. Documentation describing cryptographic configuration and weak protocol versions is available.

2547 **Assessment activities**

- 2548 1. Review documentation to identify all protocols that do not use state of the art cryptography and the available
 2549 configuration options.
 2550 2. Use the configuration interface to disable a protocol that does not use state of the art cryptography, where the
 2551 documentation states disabling is operationally feasible. Verify the product refuses a connection using the
 2552 disabled protocol.
 2553 3. Disable a weak protocol version using the configuration interface. Verify that the strong protocol version
 2554 continues to function by completing a management session using it.
 2555 4. Verify that the documentation provides a justification for each weak protocol version where disabling is not
 2556 operationally feasible.

2557 **Assessment verdict**

2558 The verdict fail is assigned if any of the following conditions apply:

- 2559 1. Documentation does not describe all protocols that do not use state of the art cryptography and the available
 2560 configuration options.
 2561 2. The product does not provide configuration options to disable protocols that do not use state of the art
 2562 cryptography where operationally feasible.
 2563 3. The product does not refuse connections on disabled protocols.
 2564 4. The product does not continue to support strong protocol versions after weak versions are disabled.
 2565 5. Documentation does not list a justification for each weak protocol version where disabling is not operationally
 2566 feasible.

2567 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2568 1. Documentation describes all protocols that do not use state of the art cryptography and the available
 2569 configuration options.
 2570 2. The product provides configuration options to disable protocols that do not use state of the art cryptography
 2571 where operationally feasible.
 2572 3. The product refuses connections on disabled protocols.

- 2573 4. The product continues to support strong protocol versions after weak versions are disabled.
 2574 5. Documentation lists a justification for each weak protocol version where disabling is not operationally feasible.

2575 **Assessment evidence**

- 2576 1. Documentation describing all protocols that do not use state of the art cryptography and the available
 2577 configuration options.
 2578 2. Test results showing the product provides configuration options to disable protocols that do not use state of the
 2579 art cryptography where operationally feasible.
 2580 3. Test results showing the product refuses connections on disabled protocols.
 2581 4. Test results showing the strong protocol version continues to function after weak versions are disabled.
 2582 5. Documentation listing a justification for each weak protocol version where disabling is not operationally
 2583 feasible.
 2584

2585 [\[AC-AUTH-4-04\]](#) Verify that the product validates trust establishment using additional mechanisms and generates audit
 2586 events for all trust relationship changes.

2587 **Assessment reference**

2588 Requirement [\[RO-AUTH-4-04\]](#).

2589 **Assessment objective**

2590 Confirm that the product validates trust establishment using additional mechanisms and that the product generates audit
 2591 events for all trust relationship changes.

2592 **Assessment preparation**

- 2593 1. The product is in product operational state.
 2594 2. Documentation describing trust establishment protocols and validation mechanisms is available.

2595 **Assessment activities**

- 2596 1. Review documentation to identify protocols that establish trust without cryptographic verification and the
 2597 additional validation mechanisms for each.
 2598 2. Trigger a trust establishment event for each identified protocol. Verify the additional validation mechanism
 2599 operates.
 2600 3. Attempt to establish a trust relationship through a spoofed source or a source without authorization. Verify the
 2601 validation mechanism detects or mitigates the attempt.
 2602 4. Verify that the product generates audit events for all trust relationship changes.

2603 **Assessment verdict**

2604 The verdict fail is assigned if any of the following conditions apply:

- 2605 1. Documentation does not list trust establishment protocols or their additional validation mechanisms.
 2606 2. The product does not operate additional validation mechanisms during trust establishment events.
 2607 3. The product does not detect or mitigate spoofed trust establishment attempts via validation mechanisms.
 2608 4. The product does not generate audit events for all trust relationship changes.

2609 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2610 1. Documentation lists trust establishment protocols and their additional validation mechanisms.
 2611 2. The product operates additional validation mechanisms during trust establishment events.
 2612 3. The product detects or mitigates spoofed trust establishment attempts via validation mechanisms.
 2613 4. The product generates audit events for all trust relationship changes.

2614 **Assessment evidence**

- 2615 1. Documentation listing trust establishment protocols and their additional validation mechanisms.
 2616 2. Test results showing additional validation mechanisms operate during trust establishment events.
 2617 3. Test results showing the product detects or mitigates spoofed trust establishment attempts via validation
 2618 mechanisms.
 2619 4. Test results showing audit events are generated for all trust relationship changes.

2620

2621

6.6 Data protection

2622

6.6.1 Requirement assessments

2623 [\[AC-DATA-1-01\]](#) Verify that the product encrypts data at rest using state of the art cryptography.2624 **Assessment reference**2625 Requirement [\[RQ-DATA-1-01\]](#).2626 **Assessment objective**

2627 Confirm that the product encrypts data at rest using state of the art cryptography.

2628 **Assessment preparation**

- 2629 1. The product is in product operational state with at least one user account configured.
- 2630 2. Documentation describing data stored by the product and the protection applied is available.

2631 **Assessment activities**

- 2632 1. Review documentation to identify all categories of data stored by the product and the protection applied to
- 2633 each. Verify the documented cryptography is state of the art.
- 2634 2. Configure a known password, credential, and where feasible a known cryptographic key. Inspect storage to
- 2635 verify the stored representation is not plaintext and is consistent with the documented protection.

2636 **Assessment verdict**

2637 The verdict fail is assigned if any of the following conditions apply:

- 2638 1. Documentation does not list all categories of data stored by the product and their storage protection.
- 2639 2. The product does not use state of the art cryptography for data storage.
- 2640 3. The product stores any data in plaintext.
- 2641 4. Any stored representation is not consistent with the documented protection.

2642 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2643 1. Documentation lists all categories of data stored by the product and their storage protection.
- 2644 2. The product uses state of the art cryptography for data storage.
- 2645 3. The product does not store any data in plaintext.
- 2646 4. All stored representations are consistent with the documented protection.

2647 **Assessment evidence**

- 2648 1. Documentation listing all categories of data stored by the product and their storage protection.
- 2649 2. Test results showing the data storage uses state of the art cryptography.
- 2650 3. Test results showing the product does not store any data in plaintext.
- 2651 4. Test results showing all stored representations are consistent with the documented protection.

2652

2653 [\[AC-DATA-1-02\]](#) Verify that the product encrypts management communications and control plane traffic using state of
2654 the art cryptography.2655 **Assessment reference**2656 Requirement [\[RQ-DATA-1-02\]](#).2657 **Assessment objective**2658 Confirm that the product encrypts management communications and control plane traffic using state of the art
2659 cryptography.2660 **Assessment preparation**

- 2661 1. The product is in product operational state with management and control plane traffic actively flowing.
- 2662 2. Documentation describing management communication channels and control plane protocols is available.

2663 **Assessment activities**

- 2664 1. Review documentation to identify all management communication channels and control plane protocols.
 2665 Verify the documented cryptography is state of the art.
- 2666 2. Inspect network traffic during active management and control plane exchanges. Verify the captured traffic uses
 2667 state of the art cryptography.
- 2668 3. Attempt to disable encryption for management communications and control plane traffic. Verify the product
 2669 does not permit this silently or without documented justification.

2670 **Assessment verdict**

2671 The verdict fail is assigned if any of the following conditions apply:

- 2672 1. Documentation does not list all management channels or control plane protocols.
- 2673 2. The product does not use state of the art cryptography for any management channel or control plane protocol.
- 2674 3. The product does not use state of the art cryptography for management communications or control plane
 2675 traffic.
- 2676 4. The product permits encryption for management communications to be disabled.
- 2677 5. The product permits encryption for control plane traffic to be disabled.

2678 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2679 1. Documentation lists all management channels and control plane protocols.
- 2680 2. The product uses state of the art cryptography for all management channels and control plane protocols.
- 2681 3. The product uses state of the art cryptography for management communications and control plane traffic.
- 2682 4. The product does not permit encryption for management communications to be disabled.
- 2683 5. The product does not permit encryption for control plane traffic to be disabled.

2684 **Assessment evidence**

- 2685 1. Documentation listing all management channels and control plane protocols.
- 2686 2. Test results showing state of the art cryptography for all management channels and control plane protocols.
- 2687 3. Test results from network traffic captures during management and control plane exchanges showing state of
 2688 the art cryptography.
- 2689 4. Test results showing the product does not permit encryption for management communications to be disabled.
- 2690 5. Test results showing the product does not permit encryption for control plane traffic to be disabled.
- 2691

2692 [\[AC-DATA-1-03\]](#) Verify that the product prevents modification of configuration and firmware without authorization.

2693 **Assessment reference**

2694 Requirement [\[RO-DATA-1-03\]](#).

2695 **Assessment objective**

2696 Confirm that the product prevents modification of configuration and firmware without authorization.

2697 **Assessment preparation**

- 2698 1. The product is in product operational state.
- 2699 2. Documentation describing the integrity verification mechanisms for configuration files and firmware images is
 2700 available.

2701 **Assessment activities**

- 2702 1. Review documentation to identify the integrity verification mechanisms and the authorization level required
 2703 for modification of each.
- 2704 2. Attempt to modify a configuration file using an authorized account. Verify that the modification succeeds.
- 2705 3. Attempt to modify a configuration file using an insufficiently privileged account. Verify the modification is
 2706 denied.
- 2707 4. Modify a configuration file directly on the storage medium where direct storage access is feasible. Verify the
 2708 product detects, rejects, or reverts the modification.
- 2709 5. Attempt to install a tampered firmware image. Verify that the product detects the modification and rejects
 2710 installation.

2711 6. Install the valid firmware image using an authorized account. Verify installation succeeds.

2712 **Assessment verdict**

2713 The verdict fail is assigned if any of the following conditions apply:

- 2714 1. Documentation does not describe integrity verification mechanisms for configuration files or firmware images.
- 2715 2. Documentation does not describe the authorization level required for modification of each.
- 2716 3. The product does not accept configuration modifications by authorized accounts.
- 2717 4. The product does not deny configuration modifications by insufficiently privileged accounts.
- 2718 5. The product does not detect or prevent direct storage modification of configuration files.
- 2719 6. The product does not detect and reject tampered firmware images.
- 2720 7. The product does not install valid firmware successfully with an authorized account.

2721 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2722 1. Documentation describes integrity verification mechanisms for configuration files and firmware images.
- 2723 2. Documentation describes the authorization level required for modification of each.
- 2724 3. The product accepts configuration modifications by authorized accounts.
- 2725 4. The product denies configuration modifications by insufficiently privileged accounts.
- 2726 5. The product detects or prevents direct storage modification of configuration files.
- 2727 6. The product detects and rejects tampered firmware images.
- 2728 7. The product installs valid firmware successfully with an authorized account.

2729 **Assessment evidence**

- 2730 1. Documentation describing the integrity verification mechanisms for configuration files and firmware images.
- 2731 2. Documentation describing the authorization level required for modification of each.
- 2732 3. Test results showing the product accepts configuration modifications by authorized accounts.
- 2733 4. Test results showing the product denies configuration modifications by insufficiently privileged accounts.
- 2734 5. Test results showing that direct storage modification of configuration files is detected or rejected where feasible.
- 2735 6. Test results showing that the product detects and rejects a tampered firmware image.
- 2736 7. Test results showing that valid firmware installation succeeds with an authorized account.

2738

2739 [\[AC-DATA-1-04\]](#) Verify that the product restricts processing and retention to the minimum that is required for its
2740 intended functions.

2741 **Assessment reference**

2742 Requirement [\[RQ-DATA-1-04\]](#).

2743 **Assessment objective**

2744 Confirm that the product restricts data processing and retention to the minimum that is required for its intended
2745 functions.

2746 **Assessment preparation**

- 2747 1. The product is in product operational state.
- 2748 2. Documentation describing the intended product functions and data processing requirements is available.

2749 **Assessment activities**

- 2750 1. Review documentation to identify the intended product functions and the categories of data that each function
2751 processes and retains.
- 2752 2. Attempt to retrieve retained data through the product. Verify data categories are consistent with documented
2753 intended functions.
- 2754 3. Capture outbound network traffic during operation. Verify the product transmits only data consistent with
2755 documented intended functions.

2756 **Assessment verdict**

2757 The verdict fail is assigned if any of the following conditions apply:

- 2758 1. Documentation does not list the intended product functions and the categories of data processed and retained
 2759 for each.
 2760 2. The product does not restrict retained data to categories consistent with documented intended functions.
 2761 3. The product does not restrict transmitted data to categories consistent with documented intended functions.

2762 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2763 1. Documentation lists the intended product functions and the categories of data processed and retained for each.
 2764 2. The product restricts retained data to categories consistent with documented intended functions.
 2765 3. The product restricts transmitted data to categories consistent with documented intended functions.

2766 **Assessment evidence**

- 2767 1. Documentation listing the intended product functions and the categories of data that each function processes
 2768 and retains.
 2769 2. Test results showing the product restricts retained data to categories consistent with documented intended
 2770 functions.
 2771 3. Test results from traffic capture confirming transmitted data is consistent with documented intended functions.
 2772

2773 **6.7 Availability protection**

2774 **6.7.1 Requirement assessments**

2775 [\[AC-AVAIL-1-01\]](#) Verify that the product enforces rate limiting for each network protocol terminated by the product.

2776 **Assessment reference**

2777 Requirement [\[RO-AVAIL-1-01\]](#).

2778 **Assessment objective**

2779 Confirm that the product enforces rate limiting for each network protocol terminated by the product.

2780 **Assessment preparation**

- 2781 1. The product is in product operational state with at least one network protocol actively handling traffic.
 2782 2. Documentation describing the rate limiting mechanisms and their configured thresholds and parameters is
 2783 available.

2784 **Assessment activities**

- 2785 1. Review documentation to identify all rate limiting mechanisms, protected protocols, and their configured
 2786 thresholds and parameters.
 2787 2. Send legitimate traffic through the product at normal rates and record baseline throughput, response time, and
 2788 resource utilization.
 2789 3. Send requests to a protected protocol at a rate exceeding the documented threshold. Verify the product begins
 2790 rejecting or delaying excess requests and that the documented threshold and time window match the observed
 2791 enforcement point.
 2792 4. Initiate a simulated traffic flood against the product from one source and simultaneously send legitimate traffic
 2793 from a separate source. Verify that throughput and response time for the legitimate traffic confirm it continues
 2794 to be processed and that essential forwarding and management functions remain operational.

2795 **Assessment verdict**

2796 The verdict fail is assigned if any of the following conditions apply:

- 2797 1. Documentation does not list all rate limiting mechanisms, protected protocols, thresholds, and parameters.
 2798 2. The product does not maintain stable throughput, response time, or resource utilization under normal traffic.
 2799 3. The product does not implement rate limiting.
 2800 4. The product does not enforce the documented rate limiting thresholds.
 2801 5. The product does not reject or delay excess requests beyond rate limiting thresholds.
 2802 6. The product does not enforce a rate limiting time window that matches the documented value.
 2803 7. The product does not continue to process legitimate traffic during simulated attack.

2804 8. The product does not maintain essential forwarding and management functions during attack.

2805 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2806 1. Documentation lists all rate limiting mechanisms, protected protocols, thresholds, and parameters.
- 2807 2. The product maintains stable throughput, response time, and resource utilization under normal traffic.
- 2808 3. The product implements rate limiting.
- 2809 4. The product enforces the documented rate limiting thresholds.
- 2810 5. The product rejects or delays excess requests beyond rate limiting thresholds.
- 2811 6. The product enforces a rate limiting time window that matches the documented value.
- 2812 7. The product continues to process legitimate traffic during simulated attack.
- 2813 8. The product maintains essential forwarding and management functions during attack.

2814 **Assessment evidence**

- 2815 1. Documentation listing all rate limiting mechanisms, protected protocols, thresholds, and parameters.
- 2816 2. Test results showing baseline throughput, response time, and resource utilization are recorded.
- 2817 3. Test results showing the product implements rate limiting.
- 2818 4. Test results showing the product enforces the documented rate limiting thresholds.
- 2819 5. Test results showing the product rejects or delays excess requests beyond rate limiting thresholds.
- 2820 6. Test results showing the observed rate limiting time window matches the documented value.
- 2821 7. Test results showing legitimate traffic continues to be processed during simulated attack.
- 2822 8. Test results showing forwarding and management functions remain operational during attack.

2823

2824 [\[AC-AVAIL-1-02\]](#) Verify that the product enforces connection throttling for each connection-oriented network protocol
 2825 terminated by the product.

2826 **Assessment reference**

2827 Requirement [\[RQ-AVAIL-1-02\]](#).

2828 **Assessment objective**

2829 Confirm that the product enforces connection throttling for each connection-oriented network protocol terminated by
 2830 the product.

2831 **Assessment preparation**

- 2832 1. The product is in product operational state with at least one connection-establishing network protocol actively
 2833 handling traffic.
- 2834 2. Documentation describing the connection throttling mechanisms and their configured parameters is available.

2835 **Assessment activities**

- 2836 1. Review documentation to identify all connection throttling mechanisms, protected protocols, and their
 2837 configured parameters.
- 2838 2. Initiate new connections to the product at a rate exceeding the documented connection throttling parameter.
 2839 Verify the product limits new connections.

2840 **Assessment verdict**

2841 The verdict fail is assigned if any of the following conditions apply:

- 2842 1. Documentation does not list all connection throttling mechanisms, protected protocols, and parameters.
- 2843 2. The product does not implement connection throttling.
- 2844 3. The product does not enforce the documented connection throttling parameters.
- 2845 4. The product does not limit excess connections beyond throttling parameters.

2846 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2847 1. Documentation lists all connection throttling mechanisms, protected protocols, and parameters.
- 2848 2. The product implements connection throttling.
- 2849 3. The product enforces the documented connection throttling parameters.
- 2850 4. The product limits excess connections beyond throttling parameters.

2851 **Assessment evidence**

- 2852 1. Documentation listing all connection throttling mechanisms, protected protocols, and parameters.
- 2853 2. Test results showing the product implements connection throttling.
- 2854 3. Test results showing the product enforces the documented connection throttling parameters.
- 2855 4. Test results showing the product limits excess connections beyond throttling parameters.
- 2856

2857 [\[AC-AVAIL-1-03\]](#) Verify that the product automatically recovers when DoS conditions cease, without requiring
2858 manual intervention.

2859 **Assessment reference**

2860 Requirement [\[RQ-AVAIL-1-03\]](#).

2861 **Assessment objective**

2862 Confirm that the product automatically recovers when DoS conditions cease, without requiring manual intervention,
2863 within the documented recovery time.

2864 **Assessment preparation**

- 2865 1. The product has DoS protection mechanisms activated by a simulated attack.
- 2866 2. Documentation describing automatic recovery behaviour and expected recovery time is available.

2867 **Assessment activities**

- 2868 1. Review documentation to identify the automatic recovery behaviour and expected recovery time.
- 2869 2. Initiate a simulated traffic flood to activate the DoS protection mechanisms of the product. Verify that
2870 protections are engaged, then cease the simulated attack entirely and record the cessation timestamp.
- 2871 3. Measure the time until rate limiting, connection throttling, and legitimate traffic throughput return to normal
2872 parameters after the simulated attack ceases.
- 2873 4. Verify that recovery occurred without manual intervention.
- 2874 5. Verify all essential functions are operational after recovery. Verify the product has not remained in a degraded
2875 state.

2876 **Assessment verdict**

2877 The verdict fail is assigned if any of the following conditions apply:

- 2878 1. Documentation does not describe automatic recovery behaviour and expected recovery time.
- 2879 2. The product does not activate DoS protection mechanisms when a simulated traffic flood is initiated.
- 2880 3. The product does not engage protections during the simulated traffic flood.
- 2881 4. The product does not restore rate limiting and connection throttling to normal parameters automatically.
- 2882 5. The product does not restore legitimate traffic throughput to baseline.
- 2883 6. The product does not recover within the documented recovery period.
- 2884 7. The product does not recover without manual intervention when DoS conditions cease.
- 2885 8. Any essential function does not resume normal operation after recovery.
- 2886 9. The product remains in a degraded state.

2887 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2888 1. Documentation describes automatic recovery behaviour and expected recovery time.
- 2889 2. The product activates DoS protection mechanisms when a simulated traffic flood is initiated.
- 2890 3. The product engages protections during the simulated traffic flood.
- 2891 4. The product restores rate limiting and connection throttling to normal parameters automatically.
- 2892 5. The product restores legitimate traffic throughput to baseline.
- 2893 6. The product recovers within the documented recovery period.
- 2894 7. The product recovers without manual intervention when DoS conditions cease.
- 2895 8. Each essential function resumes normal operation after recovery.
- 2896 9. The product does not remain in a degraded state.

2897 **Assessment evidence**

- 2898 1. Documentation describing automatic recovery behaviour and expected recovery time.

- 2899 2. Test results showing the product activates DoS protection mechanisms when a simulated traffic flood is
2900 initiated.
- 2901 3. Test results showing the product engages protections during the simulated traffic flood.
- 2902 4. Test results showing rate limiting and connection throttling return to normal parameters automatically after
2903 attack cessation.
- 2904 5. Test results showing legitimate traffic throughput returns to baseline after attack cessation.
- 2905 6. Test results showing recovery occurs within the documented recovery period.
- 2906 7. Test results showing recovery occurred without manual intervention when DoS conditions ceased.
- 2907 8. Test results showing all essential functions resume normal operation after recovery.
- 2908 9. Test results showing the product does not remain in a degraded state after recovery.
- 2909

2910 6.8 Impact minimisation

2911 6.8.1 Requirement assessments

2912 [\[AC-IM-1-01\]](#) Verify that the product generates audit events when (i) resource utilization exceeds the documented high
2913 utilization threshold; and (ii) resource utilization returns below the documented high utilization threshold.

2914 **Assessment reference**

2915 Requirement [\[RQ-IM-1-01\]](#).

2916 **Assessment objective**

2917 Confirm that the product generates audit events when (i) resource utilization exceeds the documented high utilization
2918 threshold; and (ii) resource utilization returns below the documented high utilization threshold.

2919 **Assessment preparation**

- 2920 1. The product is in product operational state.
- 2921 2. Documentation describing the resources monitored and their high utilization thresholds is available.

2922 **Assessment activities**

- 2923 1. Review documentation to identify the monitored resources and their high utilization thresholds.
- 2924 2. Record baseline utilization for each monitored resource and artificially increase utilization above the
2925 documented threshold for each resource.
- 2926 3. Inspect audit events. Verify that an audit event is generated for each resource that exceeds its documented high
2927 utilization threshold.
- 2928 4. Apply artificial load to drive each monitored resource above its documented high utilization threshold, then
2929 cease the load and allow utilization to return below the threshold. Inspect audit events for a threshold recovery
2930 audit event for each resource.
- 2931 5. Retrieve the audit event via the documented access interface. Verify that all utilization audit events are present
2932 and that no audit events are truncated.

2933 **Assessment verdict**

2934 The verdict fail is assigned if any of the following conditions apply:

- 2935 1. Documentation does not list monitored resources and their high utilization thresholds.
- 2936 2. Any monitored resource does not report baseline utilization.
- 2937 3. Any monitored resource does not reach utilization above the documented threshold under artificial load.
- 2938 4. The product does not generate an audit event when each monitored resource exceeds its documented high
2939 utilization threshold.
- 2940 5. The product does not generate a threshold recovery audit event when each monitored resource returns below
2941 the documented high utilization threshold.
- 2942 6. Any utilization audit event is not present in the audit log.
- 2943 7. The product does not expose audit events via the documented access interface.

2944 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 2945 1. Documentation lists monitored resources and their high utilization thresholds.

- 2946 2. Each monitored resource reports baseline utilization.
- 2947 3. Each monitored resource reaches utilization above the documented threshold under artificial load.
- 2948 4. The product generates an audit event when each monitored resource exceeds its documented high utilization
- 2949 threshold.
- 2950 5. The product generates a threshold recovery audit event when each monitored resource returns below the
- 2951 documented high utilization threshold.
- 2952 6. Each utilization audit event is present in the audit log.
- 2953 7. The product exposes audit events via the documented access interface.

2954 **Assessment evidence**

- 2955 1. Documentation listing monitored resources and their high utilization thresholds.
- 2956 2. Test results showing each monitored resource reports baseline utilization.
- 2957 3. Test results showing each monitored resource reaches utilization above the documented threshold under
- 2958 artificial load.
- 2959 4. Test results showing an audit event is generated for each resource that exceeds its high utilization threshold.
- 2960 5. Test results showing a threshold recovery audit event is generated for each resource after utilization returns
- 2961 below the documented high utilization threshold.
- 2962 6. Test results showing each utilization audit event is present in the audit log.
- 2963 7. Test results showing the product exposes audit events via the documented access interface.
- 2964

2965 **6.9 Attack surface and mitigation**

2966 **6.9.1 [INTEGRITY-1] System integrity and boot process**

2967 **6.9.1.1 Requirement assessments**

2968 [\[AC-INTEGRITY-1-01\]](#) Verify that the product verifies boot component integrity using state of the art cryptography.

2969 **Assessment reference**

2970 Requirement [\[RQ-INTEGRITY-1-01\]](#).

2971 **Assessment objective**

2972 Confirm that the product verifies boot component integrity using state of the art cryptography.

2973 **Assessment preparation**

- 2974 1. The product is in product factory default state with the boot process ready to be initiated.
- 2975 2. Documentation describing boot components subject to cryptographic verification is available.

2976 **Assessment activities**

- 2977 1. Review documentation to identify the boot verification scheme and failure behaviour. Verify the documented
- 2978 cryptography is state of the art.
- 2979 2. Boot the product and observe boot diagnostic output. Verify the product reports successful verification of each
- 2980 documented boot component.
- 2981 3. Modify one software boot component that is accessible for modification and attempt to boot the product.
- 2982 Verify the product detects the modification, refuses to execute the modified component, and enters the
- 2983 predefined failure state.
- 2984 4. Modify a software boot component that is accessible for modification, then restore the original. Verify the
- 2985 product completes normally after the original component is restored.
- 2986 5. Inspect the verification key storage. Verify the key is stored in the documented protected location and is not
- 2987 modifiable through normal product interfaces.

2988 **Assessment verdict**

2989 The verdict fail is assigned if any of the following conditions apply:

- 2990 1. Documentation does not list all boot components, verification scheme, and failure behaviour.
- 2991 2. The product does not use state of the art cryptography for boot component verification.

- 2992 3. Any boot component is not cryptographically verified before execution.
- 2993 4. The product does not detect or does not refuse to execute a modified boot component.
- 2994 5. The product does not enter the predefined failure state on verification failure.
- 2995 6. The product does not complete the boot process after restoring the original boot component during cryptographic verification testing.
- 2996
- 2997 7. The product does not store the verification key in the documented protected location.
- 2998 8. The product permits modification of the verification key through normal product interfaces.
- 2999 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:
- 3000 1. Documentation lists all boot components, verification scheme, and failure behaviour.
- 3001 2. The product uses state of the art cryptography for boot component verification.
- 3002 3. All boot components are cryptographically verified before execution.
- 3003 4. The product detects and refuses to execute a modified boot component.
- 3004 5. The product enters the predefined failure state on verification failure.
- 3005 6. The product completes the boot process after restoring the original boot component during cryptographic verification testing.
- 3006
- 3007 7. The product stores the verification key in the documented protected location.
- 3008 8. The product does not permit modification of the verification key through normal product interfaces.

3009 **Assessment evidence**

- 3010 1. Documentation listing all boot components, verification scheme, and failure behaviour.
- 3011 2. Test results showing the boot verification uses state of the art cryptography.
- 3012 3. Test results showing all boot components are cryptographically verified before execution.
- 3013 4. Test results showing the product detects and refuses to execute a modified boot component.
- 3014 5. Test results showing the product enters the predefined failure state on verification failure.
- 3015 6. Test results showing the product completes the boot process after restoring the original boot component during cryptographic verification testing.
- 3016
- 3017 7. Test results showing the verification key is stored in the documented protected location.
- 3018 8. Test results showing the verification key is not modifiable through normal product interfaces.
- 3019

3020 [\[AC-INTEGRITY-1-02\]](#) Verify that the product enforces a secure boot chain where (i) each stage verifies the next stage before transferring control; (ii) the initial bootloader is immutable or hardware-protected; (iii) the product enters a predefined failure state on verification failure; and (iv) only verified code executes during boot.

3021

3022

3023 **Assessment reference**

3024 Requirement [\[RQ-INTEGRITY-1-02\]](#).

3025 **Assessment objective**

3026 Confirm that the product enforces a secure boot chain where (i) each stage verifies the next stage before transferring control; (ii) the initial bootloader is immutable or hardware-protected; (iii) the product enters a predefined failure state on verification failure; and (iv) only verified code executes during boot.

3027

3028

3029 **Assessment preparation**

- 3030 1. The product is in product factory default state with the boot process ready to be initiated.
- 3031 2. Documentation describing the boot chain architecture is available.

3032 **Assessment activities**

- 3033 1. Review documentation to identify all boot stages and the verification mechanism for each stage transition.
- 3034 2. Attempt to modify the initial bootloader through software means. Verify the product rejects the modification.
- 3035 3. Inspect the storage medium where physically feasible. Verify it matches the documented protection mechanism.
- 3036
- 3037 4. Boot the product and observe boot diagnostic output. Verify each documented stage transition includes a verification step before control transfer.
- 3038
- 3039 5. Modify a component at an intermediate boot stage and attempt to boot the product. Verify the product enters the predefined failure state without executing the modified component.
- 3040
- 3041 6. Restore all components. Verify the product completes the boot process.

3042 **Assessment verdict**

3043 The verdict fail is assigned if any of the following conditions apply:

- 3044 1. Documentation does not describe all boot stages, verification mechanisms, and initial bootloader protection.
- 3045 2. The product does not prevent modification of the initial bootloader through software.
- 3046 3. The product does not store the initial bootloader using the documented protection mechanism.
- 3047 4. Any boot stage does not verify the next stage before transferring control.
- 3048 5. The product does not enter the predefined failure state on verification failure.
- 3049 6. The product executes modified components.
- 3050 7. The product does not complete the boot process after restoring all modified components.

3051 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3052 1. Documentation describes all boot stages, verification mechanisms, and initial bootloader protection.
- 3053 2. The product prevents modification of the initial bootloader through software.
- 3054 3. The product stores the initial bootloader using the documented protection mechanism.
- 3055 4. Each boot stage verifies the next stage before transferring control.
- 3056 5. The product enters the predefined failure state on verification failure.
- 3057 6. The product does not execute modified components.
- 3058 7. The product completes the boot process after restoring all modified components.

3059 **Assessment evidence**

- 3060 1. Documentation describing all boot stages, verification mechanisms, and initial bootloader protection.
- 3061 2. Test results from initial bootloader modification attempt show the product rejects modification through software.
- 3062 3. Test results from initial bootloader storage inspection show the storage matches the documented protection mechanism.
- 3063 4. Test results showing each boot stage verifies the next stage before transferring control.
- 3064 5. Test results showing the product enters the predefined failure state on verification failure.
- 3065 6. Test results showing the product does not execute modified components.
- 3066 7. Test results showing the product completes the boot process after restoring all modified components.

3070 [\[AC-INTEGRITY-1-03\]](#) Verify that the product generates audit events for all boot events including (i) boot stage progression; (ii) verification success or failure for each component; (iii) recovery mode activation; and (iv) detected bypass attempts.

3073 **Assessment reference**3074 Requirement [\[RO-INTEGRITY-1-03\]](#).3075 **Assessment objective**

3076 Confirm that the product generates audit events for all boot events including (i) boot stage progression; (ii) verification success or failure for each component; (iii) recovery mode activation; and (iv) detected bypass attempts.

3078 **Assessment preparation**

- 3079 1. The product is in product factory default state with the boot process ready to be initiated.
- 3080 2. Documentation describing audit events generated during the boot process is available.

3081 **Assessment activities**

- 3082 1. Review documentation to identify all boot-related audit events and their expected content.
- 3083 2. Boot the product and inspect audit events after boot completion. Verify an audit event is generated for each boot stage progression and for each verified boot component.
- 3084 3. Modify a software boot component that is accessible for modification to trigger a verification failure and boot the product. Verify an audit event is generated for the verification failure and that audit events are accessible after halt or recovery.
- 3085 4. Trigger recovery mode entry where the product supports recovery mode and inspect audit events. Verify an audit event is generated for recovery mode activation.

- 3090 5. Attempt a boot bypass where feasible and inspect audit events. Verify an audit event is generated for the
3091 bypass attempt.

3092 **Assessment verdict**

3093 The verdict fail is assigned if any of the following conditions apply:

- 3094 1. Documentation does not describe all boot-related audit events and their expected content.
- 3095 2. The product does not generate an audit event for any boot stage progression.
- 3096 3. The product does not generate an audit event for verification success for any boot component.
- 3097 4. The product does not generate an audit event for boot component verification failure.
- 3098 5. The product does not make audit events accessible after a verification failure boot attempt.
- 3099 6. The product does not generate an audit event for recovery mode activation where recovery mode is present.
- 3100 7. The product does not generate an audit event for bypass attempts where bypass detection is supported.

3101 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3102 1. Documentation describes all boot-related audit events and their expected content.
- 3103 2. The product generates an audit event for each boot stage progression.
- 3104 3. The product generates an audit event for verification success for each boot component.
- 3105 4. The product generates an audit event for boot component verification failure.
- 3106 5. The product makes audit events accessible after a verification failure boot attempt.
- 3107 6. The product generates an audit event for recovery mode activation where recovery mode is present.
- 3108 7. The product generates an audit event for bypass attempts where bypass detection is supported.

3109 **Assessment evidence**

- 3110 1. Documentation describing all boot-related audit events and their expected content.
- 3111 2. Test results showing an audit event is generated for each boot stage progression.
- 3112 3. Test results showing an audit event is generated for verification success for each boot component.
- 3113 4. Test results showing the product generates an audit event for boot component verification failure.
- 3114 5. Test results showing the product makes audit events accessible after a verification failure boot attempt.
- 3115 6. Test results showing the product generates an audit event for recovery mode activation where recovery mode is
3116 present.
- 3117 7. Test results showing the product generates an audit event for bypass attempts where bypass detection is
3118 supported.

3119

3120 [\[AC-INTEGRITY-1-04\]](#) Where recovery or maintenance modes are present, verify that the product requires
3121 authentication and authorization before granting access to those modes.

3122 **Assessment reference**

3123 Requirement [\[RO-INTEGRITY-1-04\]](#).

3124 **Assessment objective**

3125 Where recovery or maintenance modes are present, confirm that the product requires authentication and authorization
3126 before granting access to those modes, and that access without authentication or without authorization is denied.

3127 **Assessment preparation**

- 3128 1. The product is in product operational state.
- 3129 2. Documentation describing recovery and maintenance modes is available.

3130 **Assessment activities**

- 3131 1. Review documentation to determine whether recovery mode and maintenance mode are present and to identify
3132 the entry method and authentication requirements for each present mode.
- 3133 2. Attempt to enter each present mode without authentication. Verify access is denied.
- 3134 3. Attempt to enter each present mode using credentials below the required authorization level. Verify access is
3135 denied.
- 3136 4. Enter each present mode using credentials at the required authorization level. Verify that access is granted.

- 3137 5. Inspect the product for undocumented recovery or maintenance entry points where documentation states no
3138 such modes are present. Verify that no undocumented entry points exist.

3139 **Assessment verdict**

3140 The verdict fail is assigned if any of the following conditions apply:

- 3141 1. Documentation does not describe recovery and maintenance mode presence, entry methods, and requirements.
- 3142 2. The product does not deny access without authentication to each present mode.
- 3143 3. The product does not deny access with insufficient authorization to each present mode.
- 3144 4. The product does not grant access to any present mode with credentials at the required authorization level.
- 3145 5. The product exposes undocumented recovery or maintenance entry points.

3146 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3147 1. Documentation describes recovery and maintenance mode presence, entry methods, and requirements.
- 3148 2. The product denies access without authentication to each present mode.
- 3149 3. The product denies access with insufficient authorization to each present mode.
- 3150 4. The product grants access to each present mode with credentials at the required authorization level.
- 3151 5. The product does not expose undocumented recovery or maintenance entry points.

3152 **Assessment evidence**

- 3153 1. Documentation describing recovery and maintenance mode presence, entry methods, and authentication and
3154 authorization requirements.
- 3155 2. Test results from access without authentication attempts show access is denied for each present mode.
- 3156 3. Test results showing the product denies access with insufficient authorization to each present mode.
- 3157 4. Test results showing access is granted for each present mode with valid credentials at the required
3158 authorization level.
- 3159 5. Test results showing the product does not expose undocumented recovery or maintenance entry points.

3160

3161 **6.9.2 [PACKET-1] Default packet disposition**

3162 **6.9.2.1 Requirement assessments**

3163 [\[AC-PACKET-1-01\]](#) Verify that where the product cannot inspect traffic, the product applies the fail-secure action to
3164 that traffic.

3165 **Assessment reference**

3166 Requirement [\[RO-PACKET-1-01\]](#).

3167 **Assessment objective**

3168 Confirm that where the product cannot inspect traffic, the product applies the fail-secure action to that traffic.

3169 **Assessment preparation**

- 3170 1. The product is in product operational state with inspection rules configured.
- 3171 2. Documentation describing the fail-secure action and the conditions treated as traffic that cannot be inspected is
3172 available.
- 3173 3. Network traffic generation tools capable of exceeding inspection capacity and of exercising each inspection
3174 subsystem are available.

3175 **Assessment activities**

- 3176 1. Review documentation to identify the fail-secure action and the conditions treated as traffic that cannot be
3177 inspected.
- 3178 2. Submit traffic at a load exceeding the documented inspection capacity and verify the product applies the
3179 configured fail-secure action to the affected traffic.
- 3180 3. Trigger a failure of the deep packet inspection, signature-matching, or packet-reassembly subsystem and verify
3181 the product applies the fail-secure action to traffic that was reliant on the failed subsystem.
- 3182 4. Submit traffic to which a configured security rule requires decryption under conditions where decryption
3183 cannot be performed, and verify the product applies the configured fail-secure action to the affected traffic.

- 3184 5. Submit traffic that the product cannot classify conclusively as a known protocol or application where protocol-aware or application-aware inspection is configured, and verify the product applies the configured fail-secure action to the affected traffic.
- 3185
- 3186
- 3187 6. Configure a verdict-determination time constraint and submit traffic that cannot receive a security verdict
- 3188 within that constraint. Verify the product applies the configured fail-secure action to the affected traffic.

3189 **Assessment verdict**

3190 The verdict fail is assigned if any of the following conditions apply:

- 3191 1. Documentation does not describe the fail-secure action or the conditions treated as traffic that cannot be
- 3192 inspected.
- 3193 2. The product does not apply the configured fail-secure action to traffic when inspection capacity is exceeded.
- 3194 3. The product does not apply the configured fail-secure action to traffic when an inspection subsystem fails.
- 3195 4. The product does not apply the configured fail-secure action to traffic when security-rule-required decryption
- 3196 cannot be performed.
- 3197 5. The product does not apply the configured fail-secure action to traffic when protocol or application cannot be
- 3198 identified conclusively.
- 3199 6. The product does not apply the configured fail-secure action to traffic when a security verdict cannot be
- 3200 determined within configured time constraints.

3201 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3202 1. Documentation describes the fail-secure action and the conditions treated as traffic that cannot be inspected.
- 3203 2. The product applies the configured fail-secure action to traffic when inspection capacity is exceeded.
- 3204 3. The product applies the configured fail-secure action to traffic when an inspection subsystem fails.
- 3205 4. The product applies the configured fail-secure action to traffic when security-rule-required decryption cannot
- 3206 be performed.
- 3207 5. The product applies the configured fail-secure action to traffic when protocol or application cannot be
- 3208 identified conclusively.
- 3209 6. The product applies the configured fail-secure action to traffic when a security verdict cannot be determined
- 3210 within configured time constraints.

3211 **Assessment evidence**

- 3212 1. Documentation describing the fail-secure action and the conditions treated as traffic that cannot be inspected.
- 3213 2. Test results showing the product applies the configured fail-secure action to traffic when inspection capacity is
- 3214 exceeded.
- 3215 3. Test results showing the product applies the configured fail-secure action to traffic when an inspection
- 3216 subsystem fails.
- 3217 4. Test results showing the product applies the configured fail-secure action to traffic when security-rule-required
- 3218 decryption cannot be performed.
- 3219 5. Test results showing the product applies the configured fail-secure action to traffic when protocol or
- 3220 application cannot be identified conclusively.
- 3221 6. Test results showing the product applies the configured fail-secure action to traffic when a security verdict
- 3222 cannot be determined within configured time constraints.
- 3223

3224 [\[AC-PACKET-1-02\]](#) Verify that the product enables fail-open operation only through management override.

3225 **Assessment reference**

3226 Requirement [\[RQ-PACKET-1-02\]](#).

3227 **Assessment objective**

3228 Confirm that the product does not enable fail-open operation in product factory default state and enables fail-open

3229 operation only through management override.

3230 **Assessment preparation**

- 3231 1. The product is in product factory default state.
- 3232 2. Documentation describing the management override required to enable fail-open operation is available.
- 3233 3. A management account with sufficient privilege to enable fail-open operation is available.

3234 **Assessment activities**

- 3235 1. Review documentation to identify the management override required to enable fail-open operation and the
3236 privilege required to apply the override.
- 3237 2. Inspect the product in product factory default state and verify fail-open operation is not enabled.
- 3238 3. Attempt to enable fail-open operation without applying the management override and verify the attempt is
3239 rejected. Then apply the override using a management account with sufficient privilege and verify fail-open
3240 operation is enabled.

3241 **Assessment verdict**

3242 The verdict fail is assigned if any of the following conditions apply:

- 3243 1. Documentation does not describe the management override required to enable fail-open operation.
- 3244 2. Documentation does not describe the management privilege required to apply the override.
- 3245 3. The product enables fail-open operation in product factory default state.
- 3246 4. The product enables fail-open operation without the management override.
- 3247 5. The product does not enable fail-open operation when the management override is applied by a privileged
3248 management account.

3249 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3250 1. Documentation describes the management override required to enable fail-open operation.
- 3251 2. Documentation describes the management privilege required to apply the override.
- 3252 3. The product does not enable fail-open operation in product factory default state.
- 3253 4. The product does not enable fail-open operation without the management override.
- 3254 5. The product enables fail-open operation when the management override is applied by a privileged management
3255 account.

3256 **Assessment evidence**

- 3257 1. Documentation describing the management override required to enable fail-open operation.
- 3258 2. Documentation describing the management privilege required to apply the override.
- 3259 3. Test results showing fail-open operation is not enabled in product factory default state.
- 3260 4. Test results showing the product does not enable fail-open operation without the management override.
- 3261 5. Test results showing the product enables fail-open operation when the management override is applied.
3262

3263 [\[AC-PACKET-1-03\]](#) Verify that where stateful inspection is active, the product drops packets (i) that violate expected
3264 protocol state transitions; or (ii) that the product cannot reassemble for inspection.

3265 **Assessment reference**

3266 Requirement [\[RO-PACKET-1-03\]](#).

3267 **Assessment objective**

3268 Confirm that where stateful inspection is active, the product drops packets (i) that violate expected protocol state
3269 transitions; or (ii) that the product cannot reassemble for inspection.

3270 **Assessment preparation**

- 3271 1. The product is in product operational state with stateful inspection rules active.
- 3272 2. Documentation describing stateful inspection behaviour is available.

3273 **Assessment activities**

- 3274 1. Review documentation to identify the stateful inspection behaviour for protocol state violation and reassembly
3275 failure conditions.
- 3276 2. Send packets that violate expected TCP state transitions and verify the product drops the packets.
- 3277 3. Send fragmented traffic that cannot be fully reassembled and verify the product drops unreassembled
3278 fragments rather than forwarding them.

3279 **Assessment verdict**

3280 The verdict fail is assigned if any of the following conditions apply:

- 3281 1. Documentation does not describe stateful inspection behaviour for protocol state violations or reassembly
3282 failures.
- 3283 2. The product does not drop packets violating expected protocol state transitions.
- 3284 3. The product does not drop packets that cannot be reassembled for inspection.

3285 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3286 1. Documentation describes stateful inspection behaviour for protocol state violations and reassembly failures.
- 3287 2. The product drops packets violating expected protocol state transitions.
- 3288 3. The product drops packets that cannot be reassembled for inspection.

3289 **Assessment evidence**

- 3290 1. Documentation describing stateful inspection behaviour for protocol state violations and reassembly failures.
- 3291 2. Test results showing the product drops packets violating expected protocol state transitions.
- 3292 3. Test results showing the product drops packets that cannot be reassembled for inspection.
- 3293

3294 [\[AC-PACKET-1-04\]](#) Verify that the product (i) generates security events; (ii) increments bypass counters; and (iii)
3295 blocks the traffic where explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

3296 **Assessment reference**

3297 Requirement [\[RO-PACKET-1-04\]](#).

3298 **Assessment objective**

3299 Confirm that the product (i) generates security events; (ii) increments bypass counters; and (iii) blocks the traffic where
3300 explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

3301 **Assessment preparation**

- 3302 1. The product is in product operational state with inspection rules active.
- 3303 2. Documentation describing bypass detection and response behaviour is available.

3304 **Assessment activities**

- 3305 1. Review documentation to identify the bypass detection mechanisms and response behaviour.
- 3306 2. Trigger traffic to bypass inspection and verify the product generates a security event and increments the bypass
3307 counter.
- 3308 3. Verify the product blocks bypassed traffic by default and permits it only where explicit per-flow configuration
3309 is present.

3310 **Assessment verdict**

3311 The verdict fail is assigned if any of the following conditions apply:

- 3312 1. Documentation does not describe bypass detection mechanisms, security event generation, bypass counters, or
3313 default blocking of bypassed traffic.
- 3314 2. The product does not generate a security event when traffic bypasses inspection.
- 3315 3. The product does not increment the bypass counter when traffic bypasses inspection.
- 3316 4. The product does not block bypassed traffic by default.
- 3317 5. The product permits bypassed traffic without explicit per-flow configuration.

3318 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3319 1. Documentation describes bypass detection mechanisms, security event generation, bypass counters, and
3320 default blocking of bypassed traffic.
- 3321 2. The product generates a security event when traffic bypasses inspection.
- 3322 3. The product increments the bypass counter when traffic bypasses inspection.
- 3323 4. The product blocks bypassed traffic by default.
- 3324 5. The product does not permit bypassed traffic without explicit per-flow configuration.

3325 **Assessment evidence**

- 3326 1. Documentation describing bypass detection mechanisms, security event generation, bypass counters, and
3327 default blocking of bypassed traffic.

- 3328 2. Test results showing the product generates a security event when traffic bypasses inspection.
 3329 3. Test results showing the product increments the bypass counter when traffic bypasses inspection.
 3330 4. Test results showing bypassed traffic is blocked by default.
 3331 5. Test results showing bypassed traffic is permitted only where explicit per-flow configuration is present.
 3332

3333 [\[AC-PACKET-1-05\]](#) Verify that the product drops packets that violate applicable protocol standards.

3334 **Assessment reference**

3335 Requirement [\[RQ-PACKET-1-05\]](#).

3336 **Assessment objective**

3337 Confirm that the product drops packets that violate applicable protocol standards.

3338 **Assessment preparation**

- 3339 1. The product is in product operational state with inspection rules active.
 3340 2. Documentation describing packet validation and dropping behaviour is available.
 3341 3. Network traffic generation tools capable of producing malformed packets are available.

3342 **Assessment activities**

- 3343 1. Review documentation to identify the packet validation criteria and dropping behaviour.
 3344 2. Send packets that violate applicable protocol standards and verify the product drops the packets.

3345 **Assessment verdict**

3346 The verdict fail is assigned if any of the following conditions apply:

- 3347 1. Documentation does not describe the packet validation criteria or dropping behaviour.
 3348 2. The product does not drop packets that violate applicable protocol standards.

3349 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3350 1. Documentation describes the packet validation criteria and dropping behaviour.
 3351 2. The product drops packets that violate applicable protocol standards.

3352 **Assessment evidence**

- 3353 1. Documentation describing the packet validation criteria and dropping behaviour.
 3354 2. Test results showing the product drops packets that violate applicable protocol standards.
 3355

3356 **6.9.3 [EXPOSURE-1] Interface and service exposure minimization**

3357 **6.9.3.1 Requirement assessments**

3358 [\[AC-EXPOSURE-1-01\]](#) Verify that the product, in its product operational state, enables only those interfaces and
 3359 services that the intended function of the product requires.

3360 **Assessment reference**

3361 Requirement [\[RQ-EXPOSURE-1-01\]](#).

3362 **Assessment objective**

3363 Confirm that the product, in product operational state, enables only those interfaces and services that the intended
 3364 function of the product requires, and that no additional interfaces or services are active.

3365 **Assessment preparation**

- 3366 1. The product is in product operational state.
 3367 2. Documentation describing the intended product function and all interfaces and services is available.

3368 **Assessment activities**

- 3369 1. Review documentation to identify all interfaces and services and their declared status.

- 3370 2. Perform a full-port network scan of the product in product operational state and compare the results against the
 3371 essential service list. Verify no undocumented or non-essential service is listening.
 3372 3. Verify legacy protocols not actively required are disabled and only documented management interfaces are
 3373 enabled.

3374 **Assessment verdict**

3375 The verdict fail is assigned if any of the following conditions apply:

- 3376 1. Documentation does not list all essential interfaces and services with justifications.
 3377 2. Any enabled interface and service in product operational state is not documented as essential for the intended
 3378 function.
 3379 3. The product exposes any undocumented or non-essential listening service.
 3380 4. The product does not disable all legacy protocols that are not actively required.
 3381 5. Any enabled management interface is not documented for user access.

3382 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3383 1. Documentation lists all essential interfaces and services with justifications.
 3384 2. All enabled interfaces and services in product operational state are documented as essential for the intended
 3385 function.
 3386 3. The product does not expose any undocumented or non-essential listening service.
 3387 4. The product disables all legacy protocols that are not actively required.
 3388 5. All enabled management interfaces are documented for user access.

3389 **Assessment evidence**

- 3390 1. Documentation listing all essential interfaces and services with justifications.
 3391 2. Test results showing all enabled interfaces and services in product operational state are documented as
 3392 essential for the intended function.
 3393 3. Test results showing the product does not expose any undocumented or non-essential listening service.
 3394 4. Test results showing legacy protocols not actively required are disabled.
 3395 5. Test results showing all enabled management interfaces are documented for user access.
 3396

3397 [\[AC-EXPOSURE-1-02\]](#) Verify that the product provides capability to selectively enable or disable individual services
 3398 and interfaces through configuration.

3399 **Assessment reference**

3400 Requirement [\[RO-EXPOSURE-1-02\]](#).

3401 **Assessment objective**

3402 Confirm that the product provides capability to selectively enable or disable individual services and interfaces through
 3403 configuration.

3404 **Assessment preparation**

- 3405 1. The product is in product operational state.
 3406 2. Documentation describing configuration options for enabling and disabling services and interfaces is available.

3407 **Assessment activities**

- 3408 1. Review documentation to identify which services and interfaces can be individually enabled or disabled.
 3409 2. Disable and re-enable at least two configurable services. Verify the product provides the capability to disable
 3410 and re-enable each through configuration.
 3411 3. Disable and re-enable at least two configurable interfaces. Verify each is not operational when disabled and
 3412 operational when re-enabled.
 3413 4. Disable one service and one interface, then restart the product. Verify disabled configuration persists and re-
 3414 enabled configuration persists after restart.

3415 **Assessment verdict**

3416 The verdict fail is assigned if any of the following conditions apply:

- 3417 1. Documentation does not list which services and interfaces are individually enabled or disabled and the
3418 configuration procedure for each.
- 3419 2. The product does not allow individual services to be disabled and re-enabled through configuration.
- 3420 3. Any disabled service is accessible or any re-enabled service is not functional.
- 3421 4. The product does not allow individual interfaces to be disabled and re-enabled through configuration.
- 3422 5. Any disabled interface remains accessible.
- 3423 6. Any re-enabled interface is not operational.
- 3424 7. The product does not maintain service or interface configuration after restart.

3425 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3426 1. Documentation lists which services and interfaces are individually enabled or disabled and the configuration
3427 procedure for each.
- 3428 2. The product allows individual services to be disabled and re-enabled through configuration.
- 3429 3. Each disabled service is inaccessible and each re-enabled service is functional.
- 3430 4. The product allows individual interfaces to be disabled and re-enabled through configuration.
- 3431 5. Each disabled interface becomes inaccessible.
- 3432 6. Each re-enabled interface becomes operational.
- 3433 7. The product maintains service and interface configuration after restart.

3434 **Assessment evidence**

- 3435 1. Documentation listing which services and interfaces are individually enabled or disabled and the configuration
3436 procedure for each.
- 3437 2. Test results showing the product allows individual services to be disabled and re-enabled through
3438 configuration.
- 3439 3. Test results showing each disabled service is inaccessible and each re-enabled service is functional.
- 3440 4. Test results showing the product allows individual interfaces to be disabled and re-enabled through
3441 configuration.
- 3442 5. Test results showing each disabled interface becomes inaccessible.
- 3443 6. Test results showing each re-enabled interface becomes operational.
- 3444 7. Test results showing the product maintains service and interface configuration after restart.
- 3445

3446 **6.10 Monitoring and logging**

3447 **6.10.1 Requirement assessments**

3448 [\[AC-LOG-1-01\]](#) Verify that the product generates audit events for authentication activities including (i) successful or
3449 failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

3450 **Assessment reference**

3451 Requirement [\[RQ-LOG-1-01\]](#).

3452 **Assessment objective**

3453 Confirm that the product generates audit events for authentication activities including (i) successful or failed
3454 authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

3455 **Assessment preparation**

- 3456 1. The product is in product operational state with at least one user account configured and authentication failure
3457 protection enabled.
- 3458 2. Documentation is available describing authentication-related audit events.

3459 **Assessment activities**

- 3460 1. Review documentation to identify all authentication-related audit event types.
- 3461 2. Trigger each documented authentication event type in sequence including (i) successful authentication; (ii)
3462 failed authentication; (iii) account lockout trigger; (iv) account lockout release; (v) successful authentication
3463 credential change; and (vi) failed authentication credential change. Verify an audit event is generated for each.
- 3464 3. Verify that all authentication audit events are accessible for review.

3465 **Assessment verdict**

3466 The verdict fail is assigned if any of the following conditions apply:

- 3467 1. Documentation does not list all authentication audit event types.
- 3468 2. The product does not generate an audit event for each documented authentication event type including
- 3469 successful authentication, failed authentication, account lockout trigger, account lockout release, and
- 3470 authentication credential change attempt.
- 3471 3. Any authentication audit event is not accessible for review.

3472 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3473 1. Documentation lists all authentication audit event types.
- 3474 2. The product generates an audit event for each documented authentication event type including successful
- 3475 authentication, failed authentication, account lockout trigger, account lockout release, and authentication
- 3476 credential change attempt.
- 3477 3. All authentication audit events are accessible for review.

3478 **Assessment evidence**

- 3479 1. Documentation listing all authentication audit event types.
- 3480 2. Test results showing an audit event is generated for each documented authentication event type triggered in
- 3481 sequence including successful authentication, failed authentication, lockout trigger, lockout release, and
- 3482 credential change attempt.
- 3483 3. Test results showing all authentication audit events are present and retrievable.

3484

3485 [\[AC-LOG-1-02\]](#) Verify that the product generates audit events for all session lifecycle activities including (i) session

3486 establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv)

3487 concurrent session limit violations.

3488 **Assessment reference**3489 Requirement [\[RQ-LOG-1-02\]](#).3490 **Assessment objective**

3491 Confirm that the product generates audit events for all session lifecycle activities including (i) session establishment

3492 with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv) concurrent

3493 session limit violations.

3494 **Assessment preparation**

- 3495 1. The product is in product operational state with at least one user account and session management configured
- 3496 with idle timeout and concurrent session limit.
- 3497 2. Documentation is available describing session lifecycle audit events.

3498 **Assessment activities**

- 3499 1. Review documentation to identify all session lifecycle audit event types.
- 3500 2. Establish a session. Verify the product generates an audit event for session establishment with source details.
- 3501 3. Terminate a session by user-initiated logout, idle timeout, and management-initiated termination. Verify the
- 3502 product generates an audit event for each session termination with reason.
- 3503 4. Attempt to use an invalid session identifier. Verify the product generates an audit event for the failed session
- 3504 validation attempt.
- 3505 5. Exceed the concurrent session limit. Verify the product generates an audit event for the concurrent session
- 3506 limit violation.
- 3507 6. Verify all session lifecycle audit events are accessible for review.

3508 **Assessment verdict**

3509 The verdict fail is assigned if any of the following conditions apply:

- 3510 1. Documentation does not list all session lifecycle audit event types.
- 3511 2. The product does not generate an audit event for session establishment with source details.
- 3512 3. The product does not generate an audit event for each session termination with reason.
- 3513 4. The product does not generate an audit event for failed session validation attempts.

- 3514 5. The product does not generate an audit event for concurrent session limit violations.
 3515 6. Any session lifecycle audit event is not accessible for review.

3516 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3517 1. Documentation lists all session lifecycle audit event types.
 3518 2. The product generates an audit event for session establishment with source details.
 3519 3. The product generates an audit event for each session termination with reason.
 3520 4. The product generates an audit event for failed session validation attempts.
 3521 5. The product generates an audit event for concurrent session limit violations.
 3522 6. All session lifecycle audit events are accessible for review.

3523 **Assessment evidence**

- 3524 1. Documentation listing all session lifecycle audit event types.
 3525 2. Test results showing the product generates an audit event for session establishment with source details.
 3526 3. Test results showing the product generates an audit event for each session termination with reason.
 3527 4. Test results showing the product generates an audit event for failed session validation attempts.
 3528 5. Test results showing the product generates an audit event for concurrent session limit violations.
 3529 6. Test results showing all session lifecycle audit events are accessible for review.
 3530

3531 [\[AC-LOG-1-03\]](#) Verify that when a command is executed without authorization, the product generates an audit event.

3532 **Assessment reference**

3533 Requirement [\[RQ-LOG-1-03\]](#).

3534 **Assessment objective**

3535 Confirm that when a command is executed without authorization, the product generates an audit event, and that this
 3536 operates consistently across all command-capable interfaces.

3537 **Assessment preparation**

- 3538 1. The product is in product operational state with accounts at multiple privilege levels configured.
 3539 2. Documentation is available describing audit events generated for command without authorization attempts.
 3540 3. A list of at least three commands requiring higher privileges than the test account possesses is available.

3541 **Assessment activities**

- 3542 1. Review documentation to identify the audit events generated for command without authorization attempts.
 3543 2. Authenticate with a lower-privilege account on the primary command interface to test audit event generation
 3544 for command without authorization by (i) attempting at least three identified higher-privilege commands; and
 3545 (ii) inspecting audit events to verify an audit event is generated for each attempt.
 3546 3. Repeat at least one command without authorization attempt on a different command-capable interface and
 3547 inspect audit events. Verify an audit event is generated and that all command authorization audit events are
 3548 accessible and not suppressed.

3549 **Assessment verdict**

3550 The verdict fail is assigned if any of the following conditions apply:

- 3551 1. Documentation does not describe the audit events generated for command without authorization attempts.
 3552 2. Any command without authorization attempt from a lower-privilege account does not generate an audit event
 3553 when attempting at least three identified higher-privilege commands.
 3554 3. The product does not generate audit events for command without authorization attempts on secondary
 3555 interfaces.
 3556 4. The product does not generate audit events consistently across all command-capable interfaces.
 3557 5. Any command authorization audit event is not accessible for review.

3558 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3559 1. Documentation describes the audit events generated for command without authorization attempts.
 3560 2. Each command without authorization attempt from a lower-privilege account generates an audit event when
 3561 attempting at least three identified higher-privilege commands.

- 3562 3. The product generates audit events for command without authorization attempts on secondary interfaces.
 3563 4. The product generates audit events consistently across all command-capable interfaces.
 3564 5. All command authorization audit events are accessible for review.

3565 **Assessment evidence**

- 3566 1. Documentation describing the audit events generated for command without authorization attempts.
 3567 2. Test results showing each command without authorization attempt from a lower-privilege account generates an
 3568 audit event when attempting higher-privilege commands.
 3569 3. Test results showing the product generates audit events for command without authorization attempts on
 3570 secondary interfaces.
 3571 4. Test results showing the product generates audit events consistently across all command-capable interfaces.
 3572 5. Test results showing all command authorization audit events are accessible for review.
 3573

3574 **6.11 Data management**

3575 **6.11.1 [TRANSFER-1] Secure data export and transfer**

3576 **6.11.1.1 Requirement assessments**

3577 [\[AC-TRANSFER-1-01\]](#) Verify that the product transfers exported and imported data over a secure channel.

3578 **Assessment reference**

3579 Requirement [\[RO-TRANSFER-1-01\]](#).

3580 **Assessment objective**

3581 Confirm that the product transfers exported and imported data over a secure channel.

3582 **Assessment preparation**

- 3583 1. The product is in product operational state.
 3584 2. Documentation describing the data transfer channels for export and import is available.

3585 **Assessment activities**

- 3586 1. Review documentation to identify the data transfer channels for export and import. Verify the documented
 3587 transfer channels use a secure channel.
 3588 2. Initiate a data export operation and capture network traffic during the transfer. Verify the captured traffic is
 3589 protected by a secure channel and that the data export completes successfully.
 3590 3. Initiate a data import operation and capture network traffic during the transfer. Verify the captured traffic is
 3591 protected by a secure channel and that the data import completes successfully.

3592 **Assessment verdict**

3593 The verdict fail is assigned if any of the following conditions apply:

- 3594 1. Documentation does not describe the data transfer channels for export and import.
 3595 2. Documentation does not describe a secure channel for data export and data import.
 3596 3. The product does not transfer exported data over a secure channel.
 3597 4. The product does not complete data export operations successfully.
 3598 5. The product does not transfer imported data over a secure channel.
 3599 6. The product does not complete data import operations successfully.

3600 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3601 1. Documentation describes the data transfer channels for export and import.
 3602 2. Documentation describes a secure channel for data export and data import.
 3603 3. The product transfers exported data over a secure channel.
 3604 4. The product completes data export operations successfully.
 3605 5. The product transfers imported data over a secure channel.
 3606 6. The product completes data import operations successfully.

3607 **Assessment evidence**

- 3608 1. Documentation describing the data transfer channels for export and import.
- 3609 2. Documentation describing a secure channel for data export and data import.
- 3610 3. Test results from network traffic captures confirming the product transfers exported data over a secure channel.
- 3611 4. Test results showing the data export operation completes successfully.
- 3612 5. Test results from network traffic captures confirming the product transfers imported data over a secure
- 3613 channel.
- 3614 6. Test results showing the data import operation completes successfully.
- 3615

3616 [\[AC-TRANSFER-1-02\]](#) Verify that the product provides capability to export encrypted data using state of the art
3617 cryptography, with encryption that is applied based on user preference.

3618 **Assessment reference**

3619 Requirement [\[RO-TRANSFER-1-02\]](#).

3620 **Assessment objective**

3621 Confirm that the product provides capability to export encrypted data using state of the art cryptography, with
3622 encryption that is applied based on user preference.

3623 **Assessment preparation**

- 3624 1. The product is in product operational state.
- 3625 2. Documentation describing the data export encryption capability is available.

3626 **Assessment activities**

- 3627 1. Review documentation to identify the data export encryption capability. Verify the product provides encrypted
3628 data export using state of the art cryptography.
- 3629 2. Perform a data export with encryption enabled and inspect the exported file. Verify that the exported file is
3630 encrypted using state of the art cryptography.
- 3631 3. Decrypt the exported data where feasible. Verify the decrypted data matches the original exported data.
- 3632 4. Perform a data export with encryption disabled where the user is permitted to export without encryption.
3633 Verify the user interface clearly presents the encryption option and requires an explicit user choice.

3634 **Assessment verdict**

3635 The verdict fail is assigned if any of the following conditions apply:

- 3636 1. Documentation does not describe the data export encryption capability.
- 3637 2. The product does not use state of the art cryptography for data export encryption.
- 3638 3. The product does not encrypt the exported file using state of the art cryptography.
- 3639 4. Any decrypted export does not match the original exported data.
- 3640 5. The product does not apply encryption based on user preference during data export.
- 3641 6. The product does not present the encryption option in the user interface.

3642 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3643 1. Documentation describes the data export encryption capability.
- 3644 2. The product uses state of the art cryptography for data export encryption.
- 3645 3. The product encrypts the exported file using state of the art cryptography.
- 3646 4. Each decrypted export matches the original exported data.
- 3647 5. The product applies encryption based on user preference during data export.
- 3648 6. The product presents the encryption option in the user interface.

3649 **Assessment evidence**

- 3650 1. Documentation describing the data export encryption capability.
- 3651 2. Test results showing the data export encryption uses state of the art cryptography.
- 3652 3. Test results from inspecting the exported file confirming the content is encrypted using state of the art
3653 cryptography.
- 3654 4. Test results showing each decrypted export matches the original exported data.

- 3655 5. Test results showing the product applies encryption based on user preference during data export.
 3656 6. Test results showing the product presents the encryption option in the user interface.

3657

3658 [\[AC-TRANSFER-1-03\]](#) Verify that the product requires management access for data export and data import operations.

3659 **Assessment reference**

3660 Requirement [\[RQ-TRANSFER-1-03\]](#).

3661 **Assessment objective**

3662 Confirm that the product requires management access for data export and data import operations.

3663 **Assessment preparation**

- 3664 1. The product is in product operational state.
 3665 2. Documentation describing access control requirements for data transfer operations is available.

3666 **Assessment activities**

- 3667 1. Review documentation to identify the access control requirements for data export and data import operations.
 3668 2. Attempt to initiate a data export operation without management access. Verify the attempt is denied.
 3669 3. Attempt to initiate a data import operation without management access. Verify the attempt is denied.
 3670 4. Authenticate with a management account and perform a data export and a data import operation. Verify both
 3671 operations complete.

3672 **Assessment verdict**

3673 The verdict fail is assigned if any of the following conditions apply:

- 3674 1. Documentation does not describe management access requirements for data export and data import operations.
 3675 2. The product does not deny data export without management access.
 3676 3. The product does not deny data import without management access.
 3677 4. The product does not permit data export with management access.
 3678 5. The product does not permit data import with management access.

3679 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3680 1. Documentation describes management access requirements for data export and data import operations.
 3681 2. The product denies data export without management access.
 3682 3. The product denies data import without management access.
 3683 4. The product permits data export with management access.
 3684 5. The product permits data import with management access.

3685 **Assessment evidence**

- 3686 1. Documentation describing management access requirements for data export and data import operations.
 3687 2. Test results showing the product denies data export without management access.
 3688 3. Test results showing the product denies data import without management access.
 3689 4. Test results showing the product permits data export with management access.
 3690 5. Test results showing the product permits data import with management access.

3691

3692 [\[AC-TRANSFER-1-04\]](#) Verify that the product generates audit events for all data export and data import operations.

3693 **Assessment reference**

3694 Requirement [\[RQ-TRANSFER-1-04\]](#).

3695 **Assessment objective**

3696 Confirm that the product generates an audit event for every data export and data import operation whether successful or
 3697 failed.

3698 **Assessment preparation**

- 3699 1. The product is in product operational state.
 3700 2. Valid data for import is available.
 3701 3. Documentation describing the audit events generated for export and import operations is available.
 3702 4. Management and non-management credentials are available.

3703 **Assessment activities**

- 3704 1. Review documentation to identify the audit events generated for export and import operations.
 3705 2. Perform a data export with management credentials and inspect the audit event. Verify an audit event is
 3706 generated for the operation.
 3707 3. Attempt a data export with non-management credentials or trigger a failure. Verify an audit event is generated
 3708 for the failed attempt.
 3709 4. Perform a data import with management credentials using valid import data and inspect the audit event. Verify
 3710 an audit event is generated for the operation.
 3711 5. Attempt a data import with non-management credentials or using invalid data. Verify an audit event is
 3712 generated for the failed attempt and that all events are accessible for review.

3713 **Assessment verdict**

3714 The verdict fail is assigned if any of the following conditions apply:

- 3715 1. Documentation does not describe the audit events generated for export and import operations.
 3716 2. Any successful export operation does not generate an audit event.
 3717 3. Any failed export attempt does not generate an audit event.
 3718 4. Any successful import operation does not generate an audit event.
 3719 5. Any failed import attempt does not generate an audit event.
 3720 6. Any import audit event is not accessible for review.

3721 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3722 1. Documentation describes the audit events generated for export and import operations.
 3723 2. Each successful export operation generates an audit event.
 3724 3. Each failed export attempt generates an audit event.
 3725 4. Each successful import operation generates an audit event.
 3726 5. Each failed import attempt generates an audit event.
 3727 6. All import audit events are accessible for review.

3728 **Assessment evidence**

- 3729 1. Documentation describing the audit events generated for export and import operations.
 3730 2. Test results from audit event inspection show an audit event is generated for the successful export operation.
 3731 3. Test results from audit event inspection show an audit event is generated for the failed export attempt.
 3732 4. Test results from audit event inspection show an audit event is generated for the successful import operation.
 3733 5. Test results from audit event inspection show an audit event is generated for the failed import attempt.
 3734 6. Test results showing all export and import audit events are accessible for review.
 3735

3736 6.11.2 [SIGNATURE-1] Signature update and validation

3737 6.11.2.1 Requirement assessments

3738 [\[AC-SIGNATURE-1-01\]](#) Verify that the product verifies signature database update integrity using state of the art
 3739 cryptography before installation.

3740 **Assessment reference**

3741 Requirement [\[RQ-SIGNATURE-1-01\]](#).

3742 **Assessment objective**

3743 Confirm that the product verifies signature database update integrity using state of the art cryptography before
 3744 installation.

3745 **Assessment preparation**

- 3746 1. The product is in product operational state with signature database update functionality configured.
- 3747 2. Documentation describing the signature database update integrity verification mechanism is available.

3748 **Assessment activities**

- 3749 1. Review documentation to identify the signature database update integrity verification mechanism.
- 3750 2. Attempt to install a signature database update with a valid cryptographic signature. Verify the product installs it.
- 3751
- 3752 3. Attempt to install a signature database update with an invalid or missing cryptographic signature. Verify the
- 3753 product rejects it.

3754 **Assessment verdict**

3755 The verdict fail is assigned if any of the following conditions apply:

- 3756 1. Documentation does not describe the signature database update integrity verification mechanism.
- 3757 2. The product does not install signature database updates with valid cryptographic signatures.
- 3758 3. The product does not reject signature database updates with invalid or missing cryptographic signatures.

3759 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3760 1. Documentation describes the signature database update integrity verification mechanism.
- 3761 2. The product installs signature database updates with valid cryptographic signatures.
- 3762 3. The product rejects signature database updates with invalid or missing cryptographic signatures.

3763 **Assessment evidence**

- 3764 1. Documentation describing the signature database update integrity verification mechanism.
- 3765 2. Test results showing the product installs signature database updates with valid cryptographic signatures.
- 3766 3. Test results showing rejection of signature database updates with invalid or missing signatures.
- 3767

3768 [\[AC-SIGNATURE-1-03\]](#) Verify that the product prevents installation of signature database versions older than the

3769 currently installed version.

3770 **Assessment reference**

3771 Requirement [\[RQ-SIGNATURE-1-03\]](#).

3772 **Assessment objective**

3773 Confirm that the product prevents rollback to older signature database versions.

3774 **Assessment preparation**

- 3775 1. The product is in product operational state with a current signature database installed.
- 3776 2. Documentation describing the signature database downgrade prevention mechanism is available.

3777 **Assessment activities**

- 3778 1. Review documentation to identify the signature database downgrade prevention mechanism.
- 3779 2. Attempt to install a signature database version older than the currently installed version. Verify the product
- 3780 rejects it.

3781 **Assessment verdict**

3782 The verdict fail is assigned if any of the following conditions apply:

- 3783 1. Documentation does not describe the signature database downgrade prevention mechanism.
- 3784 2. The product does not prevent installation of signature database versions older than the currently installed
- 3785 version.

3786 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3787 1. Documentation describes the signature database downgrade prevention mechanism.
- 3788 2. The product prevents installation of signature database versions older than the currently installed version.

3789 **Assessment evidence**

- 3790 1. Documentation describing the signature database downgrade prevention mechanism.
 3791 2. Test results showing the product prevents installation of signature database versions older than the currently
 3792 installed version.
 3793

3794 [\[AC-SIGNATURE-1-02\]](#) Verify that the product verifies signature database integrity using state of the art cryptography
 3795 before use.

3796 **Assessment reference**

3797 Requirement [\[RO-SIGNATURE-1-02\]](#).

3798 **Assessment objective**

3799 Confirm that the product verifies signature database integrity using state of the art cryptography before use.

3800 **Assessment preparation**

- 3801 1. The product is in product operational state with a signature database installed.
 3802 2. Documentation describing the signature database integrity verification mechanism is available.

3803 **Assessment activities**

- 3804 1. Review documentation to identify the signature database integrity verification mechanism.
 3805 2. Corrupt a portion of the signature database and restart the product or trigger a database reload. Verify the
 3806 product detects the corruption and does not use the corrupted database for inspection.

3807 **Assessment verdict**

3808 The verdict fail is assigned if any of the following conditions apply:

- 3809 1. Documentation does not describe the signature database integrity verification mechanism.
 3810 2. The product does not verify signature database integrity before use.

3811 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3812 1. Documentation describes the signature database integrity verification mechanism.
 3813 2. The product verifies signature database integrity before use.

3814 **Assessment evidence**

- 3815 1. Documentation describing the signature database integrity verification mechanism.
 3816 2. Test results showing the product detects signature database corruption before operational use.
 3817

3818 [\[AC-SIGNATURE-1-04\]](#) Verify that the product restores the signature database from backup when integrity
 3819 verification fails.

3820 **Assessment reference**

3821 Requirement [\[RO-SIGNATURE-1-04\]](#).

3822 **Assessment objective**

3823 Confirm that the product automatically restores a known-good signature database from backup when integrity
 3824 verification of the active database fails.

3825 **Assessment preparation**

- 3826 1. The product is in product operational state with a signature database and backup available.
 3827 2. Documentation describing the signature database backup and restoration mechanism is available.

3828 **Assessment activities**

- 3829 1. Review documentation to identify the signature database backup and restoration mechanism.
 3830 2. Corrupt the active signature database and trigger an integrity check. Verify the product restores the database
 3831 from backup and resumes inspection.

3832 **Assessment verdict**

3833 The verdict fail is assigned if any of the following conditions apply:

- 3834 1. Documentation does not describe the signature database backup and restoration mechanism.
- 3835 2. The product does not restore the signature database from backup when integrity verification fails.

3836 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3837 1. Documentation describes the signature database backup and restoration mechanism.
- 3838 2. The product restores the signature database from backup when integrity verification fails.

3839 **Assessment evidence**

- 3840 1. Documentation describing the signature database backup and restoration mechanism.
- 3841 2. Test results showing signature database restoration from backup after integrity failure.

3842

3843 [\[AC-SIGNATURE-1-05\]](#) Verify that the product preserves user-created signatures when installing manufacturer-supplied signature database updates.

3844

3845 **Assessment reference**

3846 Requirement [\[RO-SIGNATURE-1-05\]](#).

3847 **Assessment objective**

3848 Confirm that the product preserves user-created signatures when installing manufacturer-supplied signature database updates.

3849

3850 **Assessment preparation**

- 3851 1. The product is in product operational state with both manufacturer-supplied and user-created signatures configured.
- 3852
- 3853 2. Documentation describing the user-created signature preservation mechanism is available.

3854 **Assessment activities**

- 3855 1. Review documentation to identify the user-created signature preservation mechanism.
- 3856 2. Install a manufacturer-supplied signature database update. Verify that user-created signatures remain unmodified.
- 3857

3858 **Assessment verdict**

3859 The verdict fail is assigned if any of the following conditions apply:

- 3860 1. Documentation does not describe the user-created signature preservation mechanism.
- 3861 2. The product does not preserve user-created signatures after installing a manufacturer-supplied signature database update.
- 3862

3863 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3864 1. Documentation describes the user-created signature preservation mechanism.
- 3865 2. The product preserves user-created signatures after installing a manufacturer-supplied signature database update.
- 3866

3867 **Assessment evidence**

- 3868 1. Documentation describing the user-created signature preservation mechanism.
- 3869 2. Test results showing user-created signatures are preserved after a manufacturer-supplied signature database update.
- 3870

3871

3872 [\[AC-SIGNATURE-1-06\]](#) Verify that the product checks for signature database updates at configurable intervals.

3873 **Assessment reference**

3874 Requirement [\[RO-SIGNATURE-1-06\]](#).

3875 **Assessment objective**

3876 Confirm that the product checks for signature database updates at configurable intervals.

3877 **Assessment preparation**

- 3878 1. The product is in product operational state with automatic signature database updates enabled.
- 3879 2. Documentation describing the signature database update check interval configuration is available.

3880 **Assessment activities**

- 3881 1. Review documentation to identify the signature database update check interval configuration.
- 3882 2. Verify the product checks for signature database updates within the configured interval.

3883 **Assessment verdict**

3884 The verdict fail is assigned if any of the following conditions apply:

- 3885 1. Documentation does not describe the signature database update check interval configuration.
- 3886 2. The product does not check for signature database updates within the configured interval.

3887 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3888 1. Documentation describes the signature database update check interval configuration.
- 3889 2. The product checks for signature database updates within the configured interval.

3890 **Assessment evidence**

- 3891 1. Documentation describing the signature database update check interval configuration.
- 3892 2. Test results showing signature database update checks occur within the configured interval.
- 3893

3894 [\[AC-SIGNATURE-1-07\]](#) Verify that the product defers signature database updates outside configured maintenance windows.

3895

3896 **Assessment reference**

3897 Requirement [\[RO-SIGNATURE-1-07\]](#).

3898 **Assessment objective**

3899 Confirm that the product defers signature database updates outside configured maintenance windows.

3900 **Assessment preparation**

- 3901 1. The product is in product operational state with a maintenance window configured.
- 3902 2. Documentation describing the signature database update deferral mechanism is available.

3903 **Assessment activities**

- 3904 1. Review documentation to identify the signature database update deferral mechanism.
- 3905 2. Trigger a signature database update outside the configured maintenance window. Verify the product defers the update.
- 3906

3907 **Assessment verdict**

3908 The verdict fail is assigned if any of the following conditions apply:

- 3909 1. Documentation does not describe the signature database update deferral mechanism.
- 3910 2. The product does not defer signature database updates outside the configured maintenance window.

3911 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3912 1. Documentation describes the signature database update deferral mechanism.
- 3913 2. The product defers signature database updates outside the configured maintenance window.

3914 **Assessment evidence**

- 3915 1. Documentation describing the signature database update deferral mechanism.
- 3916 2. Test results showing signature database updates are deferred outside maintenance windows.
- 3917

3918 [\[AC-SIGNATURE-1-08\]](#) Verify that the product limits signature database update download bandwidth to configurable thresholds.

3919

3920 **Assessment reference**3921 Requirement [\[RQ-SIGNATURE-1-08\]](#).3922 **Assessment objective**

3923 Confirm that the product limits signature database update download bandwidth to configurable thresholds.

3924 **Assessment preparation**

- 3925 1. The product is in product operational state with signature database update bandwidth limits configured.
- 3926 2. Documentation describing the signature database update bandwidth limit configuration is available.

3927 **Assessment activities**

- 3928 1. Review documentation to identify the signature database update bandwidth limit configuration.
- 3929 2. Configure a bandwidth limit and initiate a signature database update download. Verify the download rate does not exceed the configured threshold.
- 3930 3. Inspect the default bandwidth limit. Verify the default value limits bandwidth.

3932 **Assessment verdict**

3933 The verdict fail is assigned if any of the following conditions apply:

- 3934 1. Documentation does not describe the signature database update bandwidth limit configuration.
- 3935 2. The product does not limit signature database update download bandwidth to the configured threshold.
- 3936 3. The product does not enforce a default bandwidth limit for signature database update downloads.

3937 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3938 1. Documentation describes the signature database update bandwidth limit configuration.
- 3939 2. The product limits signature database update download bandwidth to the configured threshold.
- 3940 3. The product enforces a default bandwidth limit for signature database update downloads.

3941 **Assessment evidence**

- 3942 1. Documentation describing the signature database update bandwidth limit configuration.
- 3943 2. Test results showing signature database update download bandwidth does not exceed the configured threshold.
- 3944 3. Test results showing the default bandwidth limit for signature database update downloads is enforced.

3945

3946 [\[AC-SIGNATURE-1-09\]](#) Verify that the product retries failed signature database downloads within 24 hours.3947 **Assessment reference**3948 Requirement [\[RQ-SIGNATURE-1-09\]](#).3949 **Assessment objective**

3950 Confirm that the product retries failed signature database downloads within 24 hours.

3951 **Assessment preparation**

- 3952 1. The product is in product operational state with signature database update functionality configured.
- 3953 2. Documentation describing the signature database download retry mechanism is available.

3954 **Assessment activities**

- 3955 1. Review documentation to identify the signature database download retry mechanism.
- 3956 2. Block the signature database update server and monitor retry attempts. Verify the product retries within 24 hours.

3957

3958 **Assessment verdict**

3959 The verdict fail is assigned if any of the following conditions apply:

- 3960 1. Documentation does not describe the signature database download retry mechanism.
- 3961 2. The product does not retry failed signature database downloads within 24 hours.

3962 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3963 1. Documentation describes the signature database download retry mechanism.
 3964 2. The product retries failed signature database downloads within 24 hours.

3965 **Assessment evidence**

- 3966 1. Documentation describing the signature database download retry mechanism.
 3967 2. Test results showing the product retries failed signature database downloads within 24 hours.
 3968

3969 **6.12 Remote data processing solutions**

3970 **6.12.1 Requirement assessments**

3971 [\[AC-RDPS-1-01\]](#) Verify that the manufacturer documents all remote data processing solutions on which the product
 3972 depends.

3973 **Assessment reference**

3974 Requirement [\[RQ-RDPS-1-01\]](#).

3975 **Assessment objective**

3976 Confirm that the manufacturer documents all remote data processing solutions used by the product.

3977 **Assessment preparation**

- 3978 1. Technical documentation is available.

3979 **Assessment activities**

- 3980 1. Review the technical documentation to verify that all remote data processing solutions on which the product
 3981 depends are listed.
 3982 2. Inspect the product runtime configuration and verify that every remote data processing solution the product
 3983 communicates with is listed in the technical documentation.

3984 **Assessment verdict**

3985 The verdict fail is assigned if any of the following conditions apply:

- 3986 1. The manufacturer does not document all remote data processing solutions on which the product depends.
 3987 2. The product communicates with a remote data processing solution that is not documented.

3988 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 3989 1. The manufacturer documents all remote data processing solutions on which the product depends.
 3990 2. Each remote data processing solution the product communicates with is documented.

3991 **Assessment evidence**

- 3992 1. Documentation listing all remote data processing solutions on which the product depends.
 3993 2. Test results showing every remote data processing solution the product communicates with is documented.
 3994

3995 [\[AC-RDPS-1-02\]](#) Verify that where the product communicates with a remote data processing solution, the product
 3996 protects that communication over a secure channel.

3997 **Assessment reference**

3998 Requirement [\[RQ-RDPS-1-02\]](#).

3999 **Assessment objective**

4000 Confirm that where the product communicates with a remote data processing solution, the product protects that
 4001 communication over a secure channel.

4002 **Assessment preparation**

- 4003 1. The product is in product operational state with RDPS connectivity configured.

- 4004 2. Documentation describing the secure channel mechanism used for communication with a remote data
4005 processing solution is available.

4006 **Assessment activities**

- 4007 1. Review documentation to identify the secure channel mechanism used for communication with a remote data
4008 processing solution.
4009 2. Capture network traffic between the product and a remote data processing solution. Verify the product protects
4010 the communication over a secure channel.

4011 **Assessment verdict**

4012 The verdict fail is assigned if any of the following conditions apply:

- 4013 1. Documentation does not describe the secure channel mechanism used for communication with a remote data
4014 processing solution.
4015 2. The product does not protect communication with a remote data processing solution over a secure channel.

4016 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4017 1. Documentation describes the secure channel mechanism used for communication with a remote data
4018 processing solution.
4019 2. The product protects communication with a remote data processing solution over a secure channel.

4020 **Assessment evidence**

- 4021 1. Documentation describing the secure channel mechanism used for communication with a remote data
4022 processing solution.
4023 2. Test results showing the product protects communication with a remote data processing solution over a secure
4024 channel.
4025

4026 [\[AC-RDPS-1-03\]](#) Verify that where the product communicates with a remote data processing solution, the product
4027 authenticates the remote data processing solution before transmitting data to it.

4028 **Assessment reference**

4029 Requirement [\[RO-RDPS-1-03\]](#).

4030 **Assessment objective**

4031 Confirm that where the product communicates with a remote data processing solution, the product authenticates the
4032 remote data processing solution before transmitting data to it.

4033 **Assessment preparation**

- 4034 1. The product is in product operational state with RDPS connectivity configured.
4035 2. Documentation describing the remote data processing solution authentication mechanism is available.

4036 **Assessment activities**

- 4037 1. Review documentation to identify the remote data processing solution authentication mechanism.
4038 2. Substitute the remote data processing solution with an endpoint that does not satisfy authentication. Verify the
4039 product does not transmit data to the substituted endpoint.

4040 **Assessment verdict**

4041 The verdict fail is assigned if any of the following conditions apply:

- 4042 1. Documentation does not describe the remote data processing solution authentication mechanism.
4043 2. The product does not authenticate a remote data processing solution before transmitting data to it.

4044 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4045 1. Documentation describes the remote data processing solution authentication mechanism.
4046 2. The product authenticates a remote data processing solution before transmitting data to it.

4047 **Assessment evidence**

- 4048 1. Documentation describing the remote data processing solution authentication mechanism.

4049 2. Test results showing the product authenticates a remote data processing solution before transmitting data to it.
4050

4051 [\[AC-RDPS-1-04\]](#) Verify that where the product communicates with a remote data processing solution, the product
4052 retries failed communications with the remote data processing solution within 24 hours.

4053 **Assessment reference**

4054 Requirement [\[RQ-RDPS-1-04\]](#).

4055 **Assessment objective**

4056 Confirm that where the product communicates with a remote data processing solution, the product retries failed
4057 communications with the remote data processing solution within 24 hours.

4058 **Assessment preparation**

- 4059 1. The product is in product operational state with RDPS connectivity configured.
- 4060 2. Documentation describing the retry mechanism for failed communications with a remote data processing
4061 solution is available.

4062 **Assessment activities**

- 4063 1. Review documentation to identify the retry mechanism for failed communications with a remote data
4064 processing solution.
- 4065 2. Block connectivity to the remote data processing solution and monitor the product retry attempts. Verify the
4066 product retries within 24 hours.

4067 **Assessment verdict**

4068 The verdict fail is assigned if any of the following conditions apply:

- 4069 1. Documentation does not describe the retry mechanism for failed communications with a remote data
4070 processing solution.
- 4071 2. The product does not retry failed communications with a remote data processing solution within 24 hours.

4072 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4073 1. Documentation describes the retry mechanism for failed communications with a remote data processing
4074 solution.
- 4075 2. The product retries failed communications with a remote data processing solution within 24 hours.

4076 **Assessment evidence**

- 4077 1. Documentation describing the retry mechanism for failed communications with a remote data processing
4078 solution.
- 4079 2. Test results showing the product retries failed communications with a remote data processing solution within
4080 24 hours.

4081

4082 [\[AC-RDPS-1-05\]](#) Verify that the product generates audit events for communication failures with a remote data
4083 processing solution.

4084 **Assessment reference**

4085 Requirement [\[RQ-RDPS-1-05\]](#).

4086 **Assessment objective**

4087 Confirm that the product generates audit events for communication failures with a remote data processing solution.

4088 **Assessment preparation**

- 4089 1. The product is in product operational state with RDPS connectivity configured.
- 4090 2. Documentation describing the audit events generated for communication failures with a remote data processing
4091 solution is available.

4092 **Assessment activities**

- 4093 1. Review documentation to identify the audit events generated for communication failures with a remote data
4094 processing solution.
4095 2. Trigger a communication failure with a remote data processing solution. Verify the product generates an audit
4096 event.

4097 **Assessment verdict**

4098 The verdict fail is assigned if any of the following conditions apply:

- 4099 1. Documentation does not describe the audit events generated for communication failures with a remote data
4100 processing solution.
4101 2. The product does not generate audit events for communication failures with a remote data processing solution.

4102 The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

- 4103 1. Documentation describes the audit events generated for communication failures with a remote data processing
4104 solution.
4105 2. The product generates audit events for communication failures with a remote data processing solution.

4106 **Assessment evidence**

- 4107 1. Documentation describing the audit events generated for communication failures with a remote data processing
4108 solution.
4109 2. Test results showing the product generates audit events for communication failures with a remote data
4110 processing solution.
4111

4112

4113 **Annex A (informative):**
 4114 **Relationship between the present document and the**
 4115 **requirements of EU Regulation (EU) 2024/2847 — the**
 4116 **Cyber Resilience Act**

4117 The present document has been prepared in response to the Commission’s standardization request C(2025)618 [i.3] to
 4118 deliver Harmonised Standard ETSI EN 304 636 under Regulation (EU) 2024/2847 — the Cyber Resilience Act (CRA)
 4119 [i.1].

4120 Once the present document is cited in the Official Journal of the European Union under Regulation (EU) 2024/2847,
 4121 presumption of conformity with the applicable requirements of the Cyber Resilience Act is conferred to products and
 4122 manufacturers complying with this European Standard, within the scope stated in Clause [1](#).

4123 **Table A.1: Relationship between the present document and the requirements of Regulation (EU)**
 4124 **2024/2847 [\[i.1\]](#) — the Cyber Resilience Act**

No	Description	Essential requirements of Regulation	Clause(s) of the present document	U/C	Condition
1	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	Annex I, Part I, (1)	Clause 5	U	
2	Products with digital elements shall be made available on the market without known exploitable vulnerabilities.	Annex I, Part I, (2)(a)	Clause 5.2	U	
3	Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	Annex I, Part I, (2)(b)	Clauses 5.3.1 and 5.3.2	U	
4	Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	Annex I, Part I, (2)(c)	Clause 5.4.1	U	
5	Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	Annex I, Part I, (2)(d)	Clauses 5.5.1 , 5.5.2 , 5.5.3 and 5.5.4	U	
6	Products with digital elements shall protect the confidentiality of stored,	Annex I, Part I, (2)(e)	Clause 5.6	U	

No	Description	Essential requirements of Regulation	Clause(s) of the present document	U/C	Condition
	transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by best practice mechanisms, and by using other technical means.				
7	Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions.	Annex I, Part I, (2)(f)	Clause 5.6	U	
8	Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation).	Annex I, Part I, (2)(g)	Clause 5.6	U	
9	Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against DoS attacks.	Annex I, Part I, (2)(h)	Clause 5.7	U	
10	Products with digital elements shall minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks.	Annex I, Part I, (2)(i)	Clause 5.8	U	
11	Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.	Annex I, Part I, (2)(j)	Clauses 5.9.2 and 5.9.3	U	
12	Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	Annex I, Part I, (2)(k)	Clause 5.9.1	U	
13	Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	Annex I, Part I, (2)(l)	Clause 5.10	U	
14	Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	Annex I, Part I, (2)(m)	Clauses 5.3.2 , 5.11.1 and 5.11.2	U	

4126	Key to columns:	
4127	Requirement:	
4128	No	A unique identifier for one row of the table which may be used to identify a requirement.
4129	Description	A textual reference to the requirement.
4130	Essential requirements of Regulation	
4131		Identification of article(s) defining the requirement in the Regulation.
4132	Clause(s) of the present document	
4133		Identification of clause(s) defining the requirement in the present document unless another
4134		document is referenced explicitly.
4135	Requirement Conditionality:	
4136	U/C	Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the
4137		manufacturer's claimed functionality of the equipment (C).
4138	Condition	Explains the conditions when the requirement is or is not applicable for a requirement which is
4139		classified "conditional".
4140	Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list	
4141	published in the Official Journal of the European Union. Users of the present document should consult frequently the	
4142	latest list published in the Official Journal of the European Union.	
4143	Other Union legislation may be applicable to the product(s) falling within the scope of the present document.	
4144		

4145 Annex B (informative): 4146 Security analysis

4147 B.1 General

4148 This clause provides the threat and vulnerability analysis that informed the risk factor-based security requirements
4149 defined in clause 5 of the present document.

4150 First, threats are identified in relation to the product functions described in clause 4.2, the assets described in clause
4151 4.3.2, and the capabilities described in clause 4.3.3 of clause 4 of the present document. These threats are listed in B.2.
4152 In this way, the threats described in B.2 can be connected to the product context within which they may arise.

4153 Second, the relevance of threats is assessed based on risk factors. Given the informative nature of this annex, the
4154 assessment of threat relevance is provided in B.3. This framework is used to condition requirements, where applicable,
4155 on the presence of risk factors that affect the applicability and likelihood of the corresponding threats.

4156 This threat-driven approach intends to ensure that security requirements remain proportionate to actual risk while
4157 achieving the security objectives defined by the CRA.

4158 B.2 Threat landscape

4159 B.2.1 Threats related to vulnerability handling

4160

Table B.1: Threats related to vulnerability handling

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-VH-01]	Exploitation of known vulnerabilities in security products	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-TD-01] Threat detection and pattern matching [FN-SP-01] Traffic access control and decision making [FN-SM-01] Signature and intelligence management [AS-FW-01] Security policies and rule sets [AS-FW-02] Signature databases and threat intelligence [AS-FW-03] Inspection engine state [CAP-FW-01] Deep packet inspection [CAP-FW-02] Stateful traffic analysis [CAP-FW-03] Signature-based threat detection [CAP-FW-04] Inline traffic enforcement
[T-VH-02]	Exploitation of inspection engine parsing vulnerabilities	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-TD-01] Threat detection and pattern matching [AS-FW-03] Inspection engine state [CAP-FW-01] Deep packet inspection [CAP-FW-02] Stateful traffic analysis
[T-VH-03]	State table exhaustion attacks	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-SP-01] Traffic access control and decision making [AS-FW-03] Inspection engine state [CAP-FW-02] Stateful traffic analysis [CAP-FW-04] Inline traffic enforcement

4161

4162 B.2.2 Threats related to access control and authentication

4163

Table B.2: Threats related to access control and authentication

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AC-01]	Access to management functions without authorization	<ul style="list-style-type: none"> [FN-SP-01] Traffic access control and decision making [FN-SM-01] Signature and intelligence management [AS-FW-01] Security policies and rule sets [AS-FW-02] Signature databases and threat intelligence
[T-AC-02]	Credential compromise and brute force attacks	<ul style="list-style-type: none"> [FN-SP-01] Traffic access control and decision making [AS-FW-01] Security policies and rule sets

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AC-03]	Session hijacking and replay attacks	<ul style="list-style-type: none"> [FN-SP-01] Traffic access control and decision making [AS-FW-01] Security policies and rule sets
[T-AC-04]	Privilege escalation through management interfaces	<ul style="list-style-type: none"> [FN-SP-01] Traffic access control and decision making [AS-FW-01] Security policies and rule sets
[T-AC-05]	Access through inspection interfaces without authorization	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [AS-FW-01] Security policies and rule sets [CAP-FW-04] Inline traffic enforcement

4164

4165 B.2.3 Threats related to availability and inspection bypass

4166 **Table B.3: Threats related to availability and inspection bypass**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AV-01]	Denial-of-service against security enforcement	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-SP-01] Traffic access control and decision making [AS-FW-03] Inspection engine state [CAP-FW-01] Deep packet inspection [CAP-FW-04] Inline traffic enforcement
[T-AV-02]	Inspection bypass through evasion techniques	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-TD-01] Threat detection and pattern matching [AS-FW-03] Inspection engine state [CAP-FW-01] Deep packet inspection [CAP-FW-02] Stateful traffic analysis [CAP-FW-03] Signature-based threat detection
[T-AV-03]	Fail-open exploitation during system failures	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-SP-01] Traffic access control and decision making [AS-FW-03] Inspection engine state [CAP-FW-04] Inline traffic enforcement

4167

4168 B.2.4 Threats related to integrity and tampering

4169 **Table B.4: Threats related to integrity and tampering**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-IT-01]	Firmware and boot process compromise	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-TD-01] Threat detection and pattern matching [FN-SP-01] Traffic access control and decision making [FN-SM-01] Signature and intelligence management [AS-FW-01] Security policies and rule sets [AS-FW-02] Signature databases and threat intelligence [AS-FW-03] Inspection engine state [CAP-FW-01] Deep packet inspection [CAP-FW-02] Stateful traffic analysis [CAP-FW-03] Signature-based threat detection [CAP-FW-04] Inline traffic enforcement
[T-IT-02]	Security rule and configuration tampering	<ul style="list-style-type: none"> [FN-SP-01] Traffic access control and decision making [AS-FW-01] Security policies and rule sets
[T-IT-03]	Tampered update package installation	<ul style="list-style-type: none"> [FN-TI-01] Traffic inspection and analysis [FN-TD-01] Threat detection and pattern matching [FN-SP-01] Traffic access control and decision making [FN-SM-01] Signature and intelligence management [AS-FW-01] Security policies and rule sets [AS-FW-02] Signature databases and threat intelligence [CAP-FW-01] Deep packet inspection [CAP-FW-02] Stateful traffic analysis [CAP-FW-03] Signature-based threat detection [CAP-FW-04] Inline traffic enforcement

4170

4171 B.2.5 Threats related to signature and intelligence integrity

4172 **Table B.5: Threats related to signature and intelligence integrity**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-SI-01]	Malicious signature distribution through compromised updates	<ul style="list-style-type: none"> • [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-02]	Signature database integrity compromise	<ul style="list-style-type: none"> • [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-03]	Threat intelligence poisoning	<ul style="list-style-type: none"> • [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-04]	Signature rollback enabling detection bypass	<ul style="list-style-type: none"> • [FN-TD-01] Threat detection and pattern matching • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-05]	Signature update disruption	<ul style="list-style-type: none"> • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection

4173

4174 B.2.6 Threats related to data protection

4175 **Table B.6: Threats related to data protection**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DP-01]	Credential and cryptographic material disclosure	<ul style="list-style-type: none"> • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-04] Audit event records
[T-DP-02]	Data exfiltration through export functions	<ul style="list-style-type: none"> • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-04] Audit event records
[T-DP-03]	Excessive data collection through inspection functions	<ul style="list-style-type: none"> • [FN-TI-01] Traffic inspection and analysis • [AS-FW-04] Audit event records • [CAP-FW-01] Deep packet inspection

4176

4177 B.2.7 Threats related to monitoring and visibility

4178 **Table B.7: Threats related to monitoring and visibility**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-MV-01]	Security event visibility elimination	<ul style="list-style-type: none"> • [FN-SP-01] Traffic access control and decision making • [AS-FW-04] Audit event records
[T-MV-02]	Audit trail tampering	<ul style="list-style-type: none"> • [FN-SP-01] Traffic access control and decision making • [AS-FW-04] Audit event records

4179

4180 B.2.8 Threats related to default configuration

4181 **Table B.8: Threats related to default configuration**

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DC-01]	Insecure default configuration exploitation	<ul style="list-style-type: none"> • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DC-02]	Lifecycle transition data exposure	<ul style="list-style-type: none"> • [CAP-FW-04] Inline traffic enforcement • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-04] Audit event records

4182

4183

B.2.9 Threats related to physical and deployment security

4184

Table B.9: Threats related to physical and deployment security

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-PD-01]	Physical tampering of hardware appliance	<ul style="list-style-type: none"> • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement
[T-PD-02]	Hypervisor and infrastructure compromise of virtual deployment	<ul style="list-style-type: none"> • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement

4185

4186

B.2.10 Threats related to detection disruption

4187

Table B.10: Threats related to detection disruption

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DD-01]	Disabling passive monitoring sensors	<ul style="list-style-type: none"> • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection

4188

4189

B.3 Threat assessment framework

4190

B.3.1 Introduction

4191 This clause establishes an assessment framework for the applicability of the threats described in clause [B.2](#) to specific
4192 products and deployments. Products within scope vary widely in function and deployment. Not all threats apply equally
4193 to all products; applicability depends on specific product properties and the operational environment.

4194 Each threat in [B.2](#) identifies the product functions, assets, and capabilities whose presence contributes to the threat's
4195 attack surface. This characterization is informative. It describes which product properties make a given threat relevant,
4196 but does not directly condition the applicability of requirements. Requirement applicability is governed by the risk
4197 factors defined in [B.3](#) and by feature-specific conditionals stated within individual requirements in clause [5](#).

4198 **B.3.2 Risk factors**

4199 The risk factors are organized into five categories:

- 4200 • baseline risk factors;
- 4201 • traffic inspection risk factors;
- 4202 • update and intelligence risk factors;
- 4203 • deployment architecture risk factors;
- 4204 • data operations risk factors.

4205 Where not explicitly stated otherwise, the risk factors apply equally to all use cases.

4206 **B.3.2.1 Baseline risk factors**

4207 The following risk factors arise from fundamental security properties required for all security products:

4208

Table B.11: Baseline risk factors

ID	Title	Description
[RF-B-01]	Initial deployment risk factor	This risk factor applies to all products when first deployed as vulnerabilities identified in the timespan between the product being made available on the market and its initial deployment are still present when the product is put to service for the first time.
[RF-B-02]	Lifecycle transition risk factor	This risk factor applies when products undergo decommissioning, service returns, ownership transfers, or equipment recycling, as products retaining configuration data during lifecycle transitions can expose information such as credentials, cryptographic keys, network topology, and threat detection rules to parties without authorization.
[RF-B-03]	Availability disruption risk factor	This risk factor applies to all products providing network security inspection or enforcement, as failure of the product cascades through dependent systems. The relevance of this risk factor increases when the product is deployed inline at network perimeters or segmentation boundaries.
[RF-B-04]	System integrity compromise risk factor	This risk factor applies to all products executing firmware and software, as in absence of trust anchors products cannot distinguish legitimate updates from malicious modifications.
[RF-B-05]	Packet processing risk factor	This risk factor applies to all products inspecting or forwarding network packets, as packets whose structures deviate from protocol specifications can impact the functionalities of the product by effects such as buffer overflows, memory corruption, or evasion of inspection.
[RF-B-06]	Attack surface exposure risk factor	This risk factor applies to all products with network interfaces, management functions, physical ports, and diagnostic capabilities, as every exposed interface potentially increases the attack surface of the product.
[RF-B-07]	Security event visibility risk factor	This risk factor applies to all products requiring breach detection, incident response, and compliance demonstration, as incomplete or missing audit logging reduces the ability to detect and investigate security incidents.

4209

4210 **B.3.2.2 Traffic inspection risk factors**

4211 The following risk factors arise from how products access and process network traffic:

4212

Table B.12: Traffic inspection risk factors

ID	Title	Description
[RF-TI-01]	Passive monitoring risk factor	This risk factor applies when products operate in traffic mirroring mode receiving packet copies without enforcement capability, as detected

ID	Title	Description
		threats have already reached their destinations and response depends on human intervention.
[RF-TI-02]	Inline enforcement risk factor	This risk factor applies when products operate inline with network traffic flows, as the product creates a single point of failure where all traffic passes through inspection engines.

4213

4214 **B.3.2.3 Update and intelligence risk factors**

4215 The following risk factors arise from security update and threat intelligence methods:

4216 **Table B.13: Update and intelligence risk factors**

ID	Title	Description
[RF-UI-01]	Manual update risk factor	This risk factor applies when products receive security updates through manual processes requiring administrative action, as in this case updates depend on the availability of the necessary personnel and are prone to human error and delay.
[RF-UI-02]	Automated update risk factor	This risk factor applies when products implement automated security update mechanisms, as compromised update infrastructure can distribute malicious updates to entire product fleets.
[RF-UI-03]	Threat intelligence exposure risk factor	This risk factor applies when products participate in threat intelligence sharing networks, as products can reveal defensive capabilities through contributed data and automatically incorporate external threat indicators without validation.

4217

4218 **B.3.2.4 Deployment architecture risk factors**

4219 The following risk factors arise from physical or virtual deployment forms:

4220 **Table B.14: Deployment architecture risk factors**

ID	Title	Description
[RF-DA-01]	Physical appliance risk factor	This risk factor applies when products are delivered as physical appliances, as physical access to the hardware can enable modification of firmware, extraction of cryptographic keys, or installation of hardware implants.
[RF-DA-02]	Virtual deployment risk factor	This risk factor applies when products are delivered as software without dedicated hardware, as products depend on the security of the underlying infrastructure and cannot independently verify infrastructure integrity.

4221

4222 **B.3.2.5 Data operations risk factors**

4223 The following risk factors arise from data import/export and transfer capabilities:

4224 **Table B.15: Data operations risk factors**

ID	Title	Description
[RF-DO-01]	Data transfer risk factor	This risk factor applies when products implement data export, import, or exchange capabilities, as critical security parameters can be leaked or manipulated during transfer.

4225

4226 **B.3.2.6 Remote data processing risk factors**4227 The following risk factors arise from product dependencies on remote data processing solutions. Requirements specific
4228 to these risk factors are defined in clause [5.12](#).

4229

Table B.16: Remote data processing risk factors

ID	Title	Description
[RF-RDPS-01]	Remote data processing dependency risk factor	This risk factor applies when the product depends on one or more remote data processing solutions for product functions, as compromise of the RDPS boundary can affect firewall, intrusion detection, or intrusion prevention operations across all connected product instances.

4230

4231 **B.3.3 Threat justification and mitigation**

4232 The following table maps each threat to the risk factors that affect its impact and likelihood, and to the requirements that
 4233 mitigate it:

4234

Table B.17: Threat justification and mitigation

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-VH-01]	Exploitation of known vulnerabilities in security products	[RF-B-01] [RF-B-05] [RF-UI-01]	[RQ-KEV-1-01] [RQ-KEV-1-02] [RQ-KEV-1-03] [RQ-UPDATE-1-01] [RQ-UPDATE-1-02] [RQ-DEFAULT-1-10] [RQ-DEFAULT-1-11] [RQ-EXPOSURE-1-01] [RQ-DEFAULT-1-13] [RQ-DEFAULT-1-08]
[T-VH-02]	Exploitation of inspection engine parsing vulnerabilities	[RF-B-05] [RF-TI-02]	[RQ-PACKET-1-01] [RQ-PACKET-1-03] [RQ-PACKET-1-05] [RQ-AVAIL-1-01] [RQ-DEFAULT-1-08]
[T-VH-03]	State table exhaustion attacks	[RF-B-03] [RF-TI-02]	[RQ-AVAIL-1-01] [RQ-AVAIL-1-02] [RQ-AVAIL-1-03] [RQ-PACKET-1-01] [RQ-PACKET-1-02] [RQ-DEFAULT-1-08] [RQ-IM-1-01]
[T-AC-01]	Access to management functions without authorization	[RF-B-06] [RF-RDPS-01]	[RQ-AUTH-1-01] [RQ-AUTH-1-02] [RQ-AUTH-1-03] [RQ-AUTH-1-05] [RQ-AUTH-1-06] [RQ-AUTH-2-01] [RQ-AUTH-2-02] [RQ-AUTH-2-03] [RQ-AUTH-2-04] [RQ-AUTH-4-01] [RQ-AUTH-4-02] [RQ-AUTH-4-03] [RQ-DEFAULT-1-06] [RQ-DEFAULT-1-07] [RQ-DEFAULT-1-09] [RQ-RDPS-1-03] [RQ-DEFAULT-1-08]
[T-AC-02]	Credential compromise and brute force attacks	[RF-B-06]	[RQ-AUTH-1-02] [RQ-AUTH-1-03] [RQ-AUTH-1-04] [RQ-AUTH-1-05] [RQ-AUTH-1-06] [RQ-AUTH-1-07]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-AC-03]	Session hijacking and replay attacks	[RF-B-06]	[RQ-DEFAULT-1-08] [RQ-AUTH-3-01] [RQ-AUTH-3-02] [RQ-AUTH-3-03] [RQ-AUTH-3-04] [RQ-AUTH-3-05] [RQ-AUTH-3-06] [RQ-LOG-1-02] [RQ-DEFAULT-1-08]
[T-AC-04]	Privilege escalation through management interfaces	[RF-B-06]	[RQ-DEFAULT-1-04] [RQ-DEFAULT-1-05] [RQ-AUTH-2-01] [RQ-AUTH-2-02] [RQ-AUTH-2-03] [RQ-AUTH-2-04] [RQ-DEFAULT-1-08]
[T-AC-05]	Access through inspection interfaces without authorization	[RF-B-06] [RF-TI-02]	[RQ-AUTH-4-01] [RQ-EXPOSURE-1-01] [RQ-EXPOSURE-1-02] [RQ-DEFAULT-1-08]
[T-AV-01]	Denial-of-service against security enforcement	[RF-B-03] [RF-TI-02]	[RQ-AVAIL-1-01] [RQ-AVAIL-1-02] [RQ-AVAIL-1-03] [RQ-PACKET-1-01] [RQ-PACKET-1-02] [RQ-DEFAULT-1-08] [RQ-IM-1-01]
[T-AV-02]	Inspection bypass through evasion techniques	[RF-B-05] [RF-TI-01] [RF-TI-02]	[RQ-PACKET-1-01] [RQ-PACKET-1-03] [RQ-PACKET-1-04] [RQ-PACKET-1-05] [RQ-DEFAULT-1-08]
[T-AV-03]	Fail-open exploitation during system failures	[RF-B-03] [RF-TI-02]	[RQ-PACKET-1-01] [RQ-PACKET-1-02] [RQ-PACKET-1-04] [RQ-AVAIL-1-01] [RQ-AVAIL-1-02] [RQ-DEFAULT-1-08] [RQ-IM-1-01]
[T-IT-01]	Firmware and boot process compromise	[RF-B-04] [RF-DA-01]	[RQ-INTEGRITY-1-01] [RQ-INTEGRITY-1-02] [RQ-INTEGRITY-1-03] [RQ-INTEGRITY-1-04] [RQ-DEFAULT-1-08]
[T-IT-02]	Security rule and configuration tampering	[RF-B-06] [RF-RDPS-01]	[RQ-AUTH-1-01] [RQ-AUTH-2-02] [RQ-AUTH-2-04] [RQ-AUTH-4-01] [RQ-DATA-1-03] [RQ-DEFAULT-1-07] [RQ-RDPS-1-02] [RQ-RDPS-1-03] [RQ-RDPS-1-05] [RQ-LOG-1-03] [RQ-DEFAULT-1-08]
[T-IT-03]	Tampered update package installation	[RF-B-04] [RF-UI-02]	[RQ-UPDATE-1-03] [RQ-UPDATE-1-04] [RQ-UPDATE-1-05] [RQ-UPDATE-1-06] [RQ-DEFAULT-1-08]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
			[RQ-UPDATE-1-07]
[T-SI-01]	Malicious signature distribution through compromised updates	[RF-UI-02] [RF-RDPS-01]	[RQ-SIGNATURE-1-01] [RQ-SIGNATURE-1-03] [RQ-SIGNATURE-1-02] [RQ-SIGNATURE-1-04] [RQ-RDPS-1-02] [RQ-RDPS-1-03] [RQ-DEFAULT-1-08] [RQ-UPDATE-1-07]
[T-SI-02]	Signature database integrity compromise	[RF-UI-02] [RF-UI-03]	[RQ-SIGNATURE-1-02] [RQ-SIGNATURE-1-04] [RQ-SIGNATURE-1-05] [RQ-DEFAULT-1-08]
[T-SI-03]	Threat intelligence poisoning	[RF-UI-03] [RF-RDPS-01]	[RQ-SIGNATURE-1-01] [RQ-SIGNATURE-1-05] [RQ-RDPS-1-02] [RQ-RDPS-1-03] [RQ-DEFAULT-1-08] [RQ-RDPS-1-05]
[T-SI-04]	Signature rollback enabling detection bypass	[RF-UI-02] [RF-UI-03]	[RQ-SIGNATURE-1-03] [RQ-SIGNATURE-1-02] [RQ-DEFAULT-1-08]
[T-SI-05]	Signature update disruption	[RF-UI-02] [RF-UI-01] [RF-RDPS-01]	[RQ-SIGNATURE-1-06] [RQ-SIGNATURE-1-07] [RQ-SIGNATURE-1-08] [RQ-SIGNATURE-1-09] [RQ-RDPS-1-04] [RQ-DEFAULT-1-08] [RQ-RDPS-1-05]
[T-DP-01]	Credential and cryptographic material disclosure	[RF-B-02] [RF-DO-01]	[RQ-AUTH-1-03] [RQ-AUTH-1-04] [RQ-AUTH-4-02] [RQ-AUTH-4-03] [RQ-DATA-1-01] [RQ-DATA-1-02] [RQ-RESET-1-01] [RQ-DEFAULT-1-08]
[T-DP-02]	Data exfiltration through export functions	[RF-DO-01]	[RQ-TRANSFER-1-01] [RQ-TRANSFER-1-02] [RQ-TRANSFER-1-03] [RQ-TRANSFER-1-04] [RQ-DEFAULT-1-08]
[T-DP-03]	Excessive data collection through inspection functions	[RF-TI-01] [RF-TI-02]	[RQ-DATA-1-04] [RQ-DEFAULT-1-08]
[T-MV-01]	Security event visibility elimination	[RF-B-07]	[RQ-DEFAULT-1-11] [RQ-AVAIL-1-03] [RQ-INTEGRITY-1-03] [RQ-INTEGRITY-1-04] [RQ-LOG-1-01] [RQ-LOG-1-02] [RQ-LOG-1-03] [RQ-DEFAULT-1-08]
[T-MV-02]	Audit trail tampering	[RF-B-07]	[RQ-AUTH-2-04] [RQ-LOG-1-03] [RQ-DEFAULT-1-08]
[T-DC-01]	Insecure default configuration exploitation	[RF-B-01]	[RQ-DEFAULT-1-01] [RQ-DEFAULT-1-02] [RQ-DEFAULT-1-03] [RQ-DEFAULT-1-04] [RQ-DEFAULT-1-05]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
			[RQ-DEFAULT-1-06] [RQ-DEFAULT-1-09] [RQ-DEFAULT-1-12] [RQ-DEFAULT-1-08] [RQ-DEFAULT-1-13]
[T-DC-02]	Lifecycle transition data exposure	[RF-B-02]	[RQ-RESET-1-01] [RQ-RESET-1-02] [RQ-RESET-1-03] [RQ-DEFAULT-1-08]
[T-PD-01]	Physical tampering of hardware appliance	[RF-DA-01]	[RQ-DEFAULT-1-07] [RQ-DEFAULT-1-10] [RQ-INTEGRITY-1-01] [RQ-INTEGRITY-1-02] [RQ-EXPOSURE-1-01] [RQ-DEFAULT-1-08]
[T-PD-02]	Hypervisor and infrastructure compromise of virtual deployment	[RF-DA-02]	[RQ-INTEGRITY-1-01] [RQ-INTEGRITY-1-02] [RQ-DATA-1-01] [RQ-DATA-1-03] [RQ-DEFAULT-1-08]
[T-DD-01]	Disabling passive monitoring sensors	[RF-TI-01]	[RQ-PACKET-1-01] [RQ-AVAIL-1-01] [RQ-AVAIL-1-03] [RQ-LOG-1-01] [RQ-DEFAULT-1-08]

4235