# Network Device Interpretation # 202021

## Incomplete Mappings of OEs in FW Module v1.4+Errata

**Status:** ☒ *Active* □ *Inactive*

**Date:** *7-Sep-2020*

**End of proposed Transition Period (to be updated after TR2TD process):** *7-Sep-2020*

**Type of Change:** ☒ Immediate application □ Minor change □ Major change

**Type of Document:** ☒ *Technical Decision* □ *Technical Recommendation*

**Approved by:** ☒ *Network iTC Interpretations Team* □ *Network iTC*

**Affected Document(s):** *FW Module v1.4+Errata 20200625*

**Affected Section(s):** *5.3.2, 5.3.4*

**Superseded Interpretation(s):** *None*

**Issue:**

*In NDcPPv2.2e additional assumptions and Objectives for the Operational Environment have been defined for virtualization which have not been accounted for in the corresponding mappings in sections 5.3.2 and 5.3.4 of the FW Module v1.4+Errata 20200625.*

**Resolution:**

To overcome this issue described in the issue section the tables in sections 5.3.2 and 5.3.4 shall be replaced as follows:

In section 5.3.2

*<old>*

| Objective for the Operational Environment | Assumptions and OSPs |
|---|---|
| OE.PHYSICAL | A.PHYSICAL_PROTECTION |
| OE.NO_GENERAL_PURPOSE | A.LIMITED_FUNCTIONALITY |
| OE.TRUSTED_ADMIN | A.TRUSTED_ADMINISTRATOR |
| OE.UPDATES | A.REGULAR_UPDATES |
| OE.ADMIN_CREDENTIALS_SECURE | A.ADMIN_CREDENTIALS_SECURE |
| OE.COMPONENTS_RUNNING | A.COMPONENTS_RUNNING |

| | |
|---|---|
| OE.RESIDUAL_INFORMATION | A.RESIDUAL_INFORMATION |

*</old>*

shall be replaced by

<new>

| Objective for the Operational Environment | Assumptions and OSPs |
|---|---|
| OE.PHYSICAL | A.PHYSICAL_PROTECTION |
| OE.NO_GENERAL_PURPOSE | A.LIMITED_FUNCTIONALITY |
| OE.TRUSTED_ADMIN | A.TRUSTED_ADMINISTRATOR, A.VS_TRUSTED_ADMINISTRATOR |
| OE.UPDATES | A.REGULAR_UPDATES, A.VS_REGULAR_UPDATES |
| OE.ADMIN_CREDENTIALS_SECURE | A.ADMIN_CREDENTIALS_SECURE |
| OE.COMPONENTS_RUNNING | A.COMPONENTS_RUNNING |
| OE.RESIDUAL_INFORMATION | A.RESIDUAL_INFORMATION |
| OE.VM_CONFIGURATION | A.VS_CORRECT_CONFIGURATION, A.VS_ISOLATON |

</new>

*In section 5.3.4*

*<old>*

| Assumption | Rationale for security objectives for the environment |
|---|---|
| A.PHYSICAL_PROTECTION | The assumption that the TOE is physically protected against all unauthorized access attempts is addressed by the corresponding requirement in OE.PHYSICAL. |
| A.LIMITED_FUNCTIONALITY | The assumption that the TOE does not provide any general purpose computing capabilities is addressed by the corresponding requirement in OE.NO_GENERAL_PURPOSE. |

| Assumption | Rationale for security objectives for the environment |
|---|---|
| A.TRUSTED_ADMINISTRATOR | The assumption that the Security Administrator is trusted is addressed by the corresponding requirement in OE.TRUSTED_ADMIN. |
| A.REGULAR_UPDATES | The assumption that the devices firmware and software is updated regularly is addressed by the corresponding requirement in OE.UPDATES. |
| A.ADMIN_CREDENTIALS_SECURE | The assumption that the Security Administrator's credentials are protected by the platform they are stored on is addressed by the corresponding requirement in OE.ADMIN_CREDENTIALS_SECURE. |
| A.COMPONENTS_RUNNING | The assumption that each component of a distributed system is functioning properly is satisfied by the fact that this is specified as an expectation by OE.COMPONENTS_RUNNING. |
| A.RESIDUAL_INFORMATION | The assumption that the Security Administrator must ensure that there is no unauthorized access possible for sensitive residual information is addressed by the corresponding requirement in OE.RESIDUAL_INFORMATION. |

*</old>*

shall be replaced by

<new>

| Assumption | Rationale for security objectives for the environment |
|---|---|
| A.PHYSICAL_PROTECTION | The assumption that the TOE is physically protected against all unauthorized access attempts is addressed by the corresponding requirement in OE.PHYSICAL. |

| Assumption | Rationale for security objectives for the environment |
|---|---|
| A.LIMITED_FUNCTIONALITY | The assumption that the TOE does not provide any general purpose computing capabilities is addressed by the corresponding requirement in OE.NO_GENERAL_PURPOSE. |
| A.TRUSTED_ADMINISTRATOR | The assumption that the Security Administrator is trusted is addressed by the corresponding requirement in OE.TRUSTED_ADMIN. |
| A.REGULAR_UPDATES | The assumption that the devices firmware and software is updated regularly is addressed by the corresponding requirement in OE.UPDATES. |
| A.ADMIN_CREDENTIALS_SECURE | The assumption that the Security Administrator’s credentials are protected by the platform they are stored on is addressed by the corresponding requirement in OE.ADMIN_CREDENTIALS_SECURE. |
| A.COMPONENTS_RUNNING | The assumption that each component of a distributed system is functioning properly is satisfied by the fact that this is specified as an expectation by OE.COMPONENTS_RUNNING. |
| A.RESIDUAL_INFORMATION | The assumption that the Security Administrator must ensure that there is no unauthorized access possible for sensitive residual information is addressed by the corresponding requirement in OE.RESIDUAL_INFORMATION. |
| A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only) | The assumption that the Security Administrator for the VS is trusted is addressed by the corresponding requirement in OE.TRUSTED_ADMIN. |
| A.VS_REGULAR_UPDATES (applies to vNDs only) | The assumption that the VS software is updated regularly is addressed by the corresponding requirement in OE.UPDATES. |

| Assumption | Rationale for security objectives for the environment |
|---|---|
| A.VS_ISOLATON (applies to vNDs only) | The assumption that the VS provides and is configured to provide sufficient isolation between software running in VMs on the same physical platform is addressed by the corresponding requirement in OE.VM_CONFIGURATION |
| A.VS_CORRECT_CONFIGURATION (applies to vNDs only) | The assumption that the VS and VMs are correctly configured is addressed by the corresponding requirement in OE.VM_CONFIGURATION |

</new>

**Rationale:**

*See 'Issue' section.*

*Background: NDcPPv2.2e as BasePP for the FW Modulev1.4+Errata claims among others APE_OBJ.1 which does not require mappings or rationales for Security Objectives for the TOE or the Operational Environment. Chapter 11 of CC Part3 v3.1R5 defines requirements for the evaluation of PP Configurations which includes requirements on PP Modules. And ACE_OBJ.1 just contains a pointer back to APE_OBJ.2. So instead of providing the same level of granularity for elements for PP Modules in ACE_OBJ.x as for (c)PPs in APE_OBJ.x there is only an equivalent to APE_OBJ.2 defined for PP Modules. We therefore need to provide the additional rationales and mappings from APE_OBJ.2 in the PP Module which are not required for the BasePP.*

**Further Action:**

*None*

**Action by Network iTC:**

*None*