This document highlights the high level changes that have been applied to the second version (v1.1) of the Network collaborative Protection Profile (cPP) and Supporting Document (SD). Note that this list highlights major change areas only and does not identify the numerous minor editorial, typographical and consistency modifications that have been applied.

Also note that whilst this public review focusses on the Network Device cPP and SD, all changes will be mirrored in an updated Firewall cPP and SD. All of the firewall specific SFRs and evaluation activities i.e. FFW_RUL_EXT remain unchanged from version 1.

NDcPP v1.1

- Introduction of support for Distributed TOEs
    - New Chapter 3 describing distributed TOE use-cases
    - Updates to FAU_GEN, FAU_STG_EXT, FIA_UIA_EXT, FMT_SMF, FMT_SMR, FPT_TST_EXT, FPT_TUD_EXT, FPT_STM and AGD_PRE
    - Addition of FTP_TRP/Join
    - Addition of FCO_CPC_EXT
    - Addition of FPT_ITT
    - Additional of FIA_X509_EXT.1/ITT
- Addition of FIA_AFL
- Removal of mandatory cipher selections in FCS_TLSC_EXT, FCS_TLSS_EXT. FCS_IPSEC_EXT, FCS_SSHS_EXT and FCS_SSHC_EXT
- Movement of all X.509 SFRs to be selection based (moved to Appendix B)
- Update of FCS_CKM.4
- SFR Rationale to threat mapping
- SFR Dependency Analysis

NDSD v1.1

- Introduction of support for Distributed TOEs
    - Updates to FAU_GEN, FAU_STG_EXT, FIA_UIA_EXT, FMT_SMF, FMT_SMR, FPT_TST_EXT, FPT_TUD_EXT, FPT_STM
    - Addition of FTP_TRP/Join
    - Addition of FCO_CPC_EXT
    - Addition of FPT_ITT
    - Additional of FIA_X509_EXT.1/ITT
    - Updates to Equivalency Considerations (Appendix B)
- Addition of AES-CTR specific tests
- Addition of FIA_AFL
- Updates to FCS_CKM.4
- Updates to AVA_VAN
- Updates to Vulnerability Analysis (Appendix A)

Network Interpretations Team (NIT) Request for interpretations (Rfi's)

In addition to the above changes, the following NIT Rfi's have also been implemented. Details of the NIT recommendations can be found in the Network iTC project space on OnlyOffice at https://ccusersforum.onlyoffice.com/products/projects/tmdocs.aspx?prjID=455640#1888103 (CCUF membership required)

- Rfi#2 – Make elliptic curves P-256 and P-384 optional for signature generation and signature verification
- Rfi#3 – Requirements on destruction of cryptographic keys
- Rfi#8 – Compliance to RFC5759 and RFC5280 for using CRLs
- Rfi#9 – Timing of verification of revocation status for X.509 certificates
- Rfi#10 – Handling of X.509 certificates when ssh-rsa Is used for all remote communication
- Rfi#11 – Using secp521r1 for TLS communications
- Rfi#12 – Password authentication for SSH Clients
- Rfi#14 – Transport and tunnel mode in IPsec communications
- Rfi#23 – NDcPP and SIP server with virtualisation
- Rfi#24 – Testing SSH 2^28 packets
- Rfi#26 – Testing the absence of a published hash for TOE update