

**Assurance Activity Report for Cisco Catalyst 8200 and 8500 Series Edge Routers  
(Cat8200, Cat8500)**

**Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) IOS-XE 17.6,**

**Collaborative Protection Profile for Network Devices (NDcPPv2.2e), Network Device  
Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP V1.2),  
Virtual Private Network (VPN) Gateways (MOD\_VPNGW\_V1.1)**

AAR Version 1.1, March 21, 2023

**Evaluated by:**



**2400 Research Blvd, Suite 395  
Rockville, MD 20850**

**Prepared for:**



**National Information Assurance Partnership  
Common Criteria Evaluation and Validation Scheme**

**The Developer of the TOE:**

**Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134**

**The Author of the Security Target:**

**Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134**

**The TOE Evaluation was Sponsored by:**

**Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134**

**Evaluation Personnel:**

**Rahul Joshi  
Snehal Raghunath Gaonkar**

**Common Criteria Version**

**Common Criteria Version 3.1 Revision 5**

**Common Evaluation Methodology Version**

**CEM Version 3.1 Revision 5**

# Revision History

VERSION	DATE	CHANGES
1.0	25/01/2023	Initial Release
1.1	21/03/2023	Updated vulnerability search date

# Contents

- 1 TOE Overview.....14**
  - 1.1 TOE Description ..... 14**
    - 1.1.1 Cisco Catalyst 8200 Series Edge Routers (Cat8200)..... 14
    - 1.1.2 Cisco Catalyst 8500 Series Edge Routers (Cat8500)..... 14
- 2 Assurance Activities Identification.....15**
- 3 Test Equivalency Justification .....16**
  - 3.1 OS, Processor, and Firmware Analysis ..... 16**
  - 3.2 Specification of Differences..... 17**
  - 3.3 Platform/Hardware Dependencies..... 17**
  - 3.4 Software/OS Dependencies: ..... 18**
  - 3.5 Differences in Libraries Used to Provide TOE Functionality ..... 18**
  - 3.6 TOE Management Interface Differences ..... 18**
  - 3.7 TOE Functional Differences ..... 18**
  - 3.8 MACsec Analysis..... 18**
  - 3.9 Difference Comparison ..... 18**
  - 3.10 Recommendations/Conclusions ..... 19**
- 4 Test Bed Descriptions .....20**
  - 4.1 Test Bed Details ..... 21**
  - 4.2 Test Time & Location ..... 22**
- 5 Detailed Test Cases (TSS and Guidance Activities) .....23**
  - 5.1 TSS and Guidance Activities (Auditing) ..... 23**
    - 5.1.1 FAU\_GEN.1..... 23
      - 5.1.1.1 FAU\_GEN.1 TSS 1 .....23
      - 5.1.1.2 FAU\_GEN.1 TSS 3 (VPNGWMod) .....23
      - 5.1.1.3 FAU\_GEN.1 TSS 4 (VPNGWMod) .....23
      - 5.1.1.4 FAU\_GEN.1 TSS 5 (VPNGWMod) .....24
      - 5.1.1.5 FAU\_GEN.1 Guidance 1 .....24
      - 5.1.1.6 FAU\_GEN.1 Guidance 2 .....25
      - 5.1.1.7 FAU\_GEN.1 Guidance 3 (VPNGWMod).....27
    - 5.1.2 FAU\_STG.1..... 27
      - 5.1.2.1 FAU\_STG.1 TSS 1.....27
    - 5.1.3 FAU\_STG\_EXT.1..... 28
      - 5.1.3.1 FAU\_STG\_EXT.1 TSS 1 .....28
      - 5.1.3.2 FAU\_STG\_EXT.1 TSS 2 .....28
      - 5.1.3.3 FAU\_STG\_EXT.1 TSS 3 .....29
      - 5.1.3.4 FAU\_STG\_EXT.1 TSS 4 .....29
      - 5.1.3.5 FAU\_STG\_EXT.1 TSS 5 .....30
      - 5.1.3.6 FAU\_STG\_EXT.1 Guidance 1 .....30
      - 5.1.3.7 FAU\_STG\_EXT.1 Guidance 2 .....31
      - 5.1.3.8 FAU\_STG\_EXT.1 Guidance 3 .....31
  - 5.2 TSS and Guidance Activities (Cryptographic Support) ..... 31**
    - 5.2.1 FCS\_CKM.1 ..... 32
      - 5.2.1.1 FCS\_CKM.1 TSS 1.....32

5.2.1.2	FCS_CKM.1 Guidance 1	32
5.2.1.3	FCS_CKM.1 Test/CAVP 1	32
5.2.2	FCS_CKM.1.1/IKE	33
5.2.2.1	FCS_CKM.1.1/IKE TSS 1	33
5.2.2.2	FCS_CKM.1.1/IKE Guidance 1	33
5.2.2.3	FCS_CKM.1/IKE Test/CAVP 1	34
5.2.3	FCS_CKM.2	34
5.2.3.1	FCS_CKM.2 TSS 1 [TD0580]	34
5.2.3.2	FCS_CKM.2 Guidance 1	35
5.2.3.3	FCS_CKM.2 Test/CAVP 1	35
5.2.4	FCS_CKM.4	36
5.2.4.1	FCS_CKM.4 TSS 1	36
5.2.4.2	FCS_CKM.4 TSS 2	38
5.2.4.3	FCS_CKM.4 TSS 3	39
5.2.4.4	FCS_CKM.4 TSS 4	39
5.2.4.5	FCS_CKM.4 TSS 5	39
5.2.4.6	FCS_CKM.4 Guidance 1	40
5.2.5	FCS_COP.1/DataEncryption	40
5.2.5.1	FCS_COP.1/DataEncryption TSS 1	40
5.2.5.2	FCS_COP.1/DataEncryption Guidance 1	40
5.2.5.3	FCS_COP.1/DataEncryption Test/CAVP 1	42
5.2.6	FCS_COP.1/SigGen	42
5.2.6.1	FCS_COP.1/SigGen TSS 1	42
5.2.6.2	FCS_COP.1/SigGen Guidance 1	42
5.2.6.3	FCS_COP.1/SigGen Test/CAVP 1	43
5.2.7	FCS_COP.1/Hash	43
5.2.7.1	FCS_COP.1/Hash TSS 1	43
5.2.7.2	FCS_COP.1/Hash Guidance 1	43
5.2.7.3	FCS_COP.1/Hash Test/CAVP 1	44
5.2.8	FCS_COP.1/KeyedHash	44
5.2.8.1	FCS_COP.1/KeyedHash TSS 1	44
5.2.8.2	FCS_COP.1/KeyedHash Guidance 1	45
5.2.8.3	FCS_COP.1/KeyedHash Test/CAVP 1	45
5.2.9	FCS_COP.1(1)/KeyedHashCMAC	45
5.2.9.1	FCS_COP.1(1)/KeyedHashCMAC TSS 1 [TD0466]	45
5.2.9.2	FCS_COP.1(1)/KeyedHashCMAC Test/CAVP 1 [TD0466]	46
5.2.10	FCS_COP.1(2) Cryptographic Operation (MACsec AES Data Encryption/Decryption)	46
5.2.10.1	FCS_COP.1(2) TSS 1 [TD0466]	46
5.2.10.2	FCS_COP.1(2) Test/CAVP 1 [TD0466]	47
5.2.11	FCS_RBG_EXT.1	47
5.2.11.1	FCS_RBG_EXT.1 TSS 1	47
5.2.11.2	FCS_RBG_EXT.1 Guidance 1	47
5.2.11.3	FCS_RBG_EXT.1.1 Test/CAVP 1	47
<b>5.3</b>	<b>TSS and Guidance Activities (IPsec)</b>	<b>48</b>
5.3.1	FCS_IPSEC_EXT.1	48

5.3.1.1	FCS_IPSEC_EXT.1.1 TSS 1	48
5.3.1.2	FCS_IPSEC_EXT.1.1 TSS 2	49
5.3.1.3	FCS_IPSEC_EXT.1.1 Guidance 1	50
5.3.1.4	FCS_IPSEC_EXT.1.3 TSS 1	50
5.3.1.5	FCS_IPSEC_EXT.1.3 Guidance 1	51
5.3.1.6	FCS_IPSEC_EXT.1.4 TSS 1	51
5.3.1.7	FCS_IPSEC_EXT.1.4 Guidance 1	52
5.3.1.8	FCS_IPSEC_EXT.1.5 TSS 1	52
5.3.1.9	FCS_IPSEC_EXT.1.5 TSS 2	53
5.3.1.10	FCS_IPSEC_EXT.1.5. Guidance 1	53
5.3.1.11	FCS_IPSEC_EXT.1.5. Guidance 2	54
5.3.1.12	FCS_IPSEC_EXT.1.6 TSS 1	55
5.3.1.13	FCS_IPSEC_EXT.1.6 Guidance 1	55
5.3.1.14	FCS_IPSEC_EXT.1.7 TSS 1	56
5.3.1.15	FCS_IPSEC_EXT.1.7 Guidance 1 [TD0633]	56
5.3.1.16	FCS_IPSEC_EXT.1.8 TSS 1	57
5.3.1.17	FCS_IPSEC_EXT.1.8 Guidance 1 [TD0633]	57
5.3.1.18	FCS_IPSEC_EXT.1.9 TSS 1	58
5.3.1.19	FCS_IPSEC_EXT.1.10 TSS 1	59
5.3.1.20	FCS_IPSEC_EXT.1.11 TSS 1	59
5.3.1.21	FCS_IPSEC_EXT.1.11 Guidance 1	59
5.3.1.22	FCS_IPSEC_EXT.1.12 TSS 1	60
5.3.1.23	FCS_IPSEC_EXT.1.13 TSS 1	61
5.3.1.24	FCS_IPSEC_EXT.1.13 TSS 2	61
5.3.1.25	FCS_IPSEC_EXT.1.13 Guidance 1	61
5.3.1.26	FCS_IPSEC_EXT.1.13 Guidance 2	62
5.3.1.27	FCS_IPSEC_EXT.1.13 Guidance 3	63
5.3.1.28	FCS_IPSEC_EXT.1.14 TSS 1	64
5.3.1.29	FCS_IPSEC_EXT.1.14 Guidance 1	64
<b>5.4</b>	<b>TSS and Guidance Activities (MACsec)</b>	<b>65</b>
5.4.1	FCS_MACSEC_EXT.1	65
5.4.1.1	FCS_MACSEC_EXT.1 TSS 1	65
5.4.1.2	FCS_MACSEC_EXT.1 TSS 2	65
5.4.1.3	FCS_MACSEC_EXT.1 TSS 3 [TD0553]	66
5.4.2	FCS_MACSEC_EXT.2	66
5.4.2.1	FCS_MACSEC_EXT.2 TSS 1	66
5.4.2.2	FCS_MACSEC_EXT.2 Guidance 1	67
5.4.3	FCS_MACSEC_EXT.3	67
5.4.3.1	FCS_MACSEC_EXT.3 TSS 1	67
5.4.4	FCS_MACSEC_EXT.4	68
5.4.4.1	FCS_MACSEC_EXT.4 TSS 1	68
5.4.4.2	FCS_MACSEC_EXT.4 Guidance 1	68
5.4.5	FCS_MKA_EXT.1	69
5.4.5.1	FCS_MKA_EXT.1.4 TSS 1	69
5.4.5.2	FCS_MKA_EXT.1.8 TSS 1	69
5.4.5.3	FCS_MKA_EXT.1.8 TSS 2	70
5.4.5.4	FCS_MKA_EXT.1.8 TSS 3	70
5.4.5.5	FCS_MKA_EXT.1.8 Guidance 1	71
<b>5.5</b>	<b>TSS and Guidance Activities (SSH)</b>	<b>71</b>

5.5.1	FCS_SSHS_EXT.1.....	71
5.5.1.1	FCS_SSHS_EXT.1.2 TSS 1 [TD0631] .....	71
5.5.1.2	FCS_SSHS_EXT.1.3 TSS 1 .....	72
5.5.1.3	FCS_SSHS_EXT.1.4 TSS 1 .....	72
5.5.1.4	FCS_SSHS_EXT.1.4 Guidance 1 .....	72
5.5.1.5	FCS_SSHS_EXT.1.5 TSS 1 [TD0631] .....	73
5.5.1.6	FCS_SSHS_EXT.1.5 TSS 2 .....	<b>Error! Bookmark not defined.</b>
5.5.1.7	FCS_SSHS_EXT.1.5 Guidance 1 .....	73
5.5.1.8	FCS_SSHS_EXT.1.6 TSS 1 .....	74
5.5.1.9	FCS_SSHS_EXT.1.6 Guidance 1 .....	74
5.5.1.10	FCS_SSHS_EXT.1.7 TSS 1 .....	74
5.5.1.11	FCS_SSHS_EXT.1.7 Guidance 1 .....	75
5.5.1.12	FCS_SSHS_EXT.1.8 TSS 1 .....	75
5.5.1.13	FCS_SSHS_EXT.1.8 Guidance 1 .....	75
<b>5.6</b>	<b>TSS and Guidance Activities (Identification and Authentication) .....</b>	<b>76</b>
5.6.1	FIA_AFL.1.....	76
5.6.1.1	FIA_AFL.1 TSS 1 .....	76
5.6.1.2	FIA_AFL.1 TSS 2 .....	77
5.6.1.3	FIA_AFL.1 Guidance 1 .....	77
5.6.1.4	FIA_AFL.1 Guidance 2 .....	78
5.6.2	FIA_PMG_EXT.1 .....	78
5.6.2.1	FIA_PMG_EXT.1.1 TSS 1 .....	78
5.6.2.2	FIA_PMG_EXT.1.1 Guidance 1 .....	78
5.6.3	FIA_PSK_EXT.1/MACsec.....	79
5.6.3.1	FIA_PSK_EXT.1/MACsec TSS 1 .....	79
5.6.3.2	FIA_PSK_EXT.1/MACsec Guidance 1.....	80
5.6.3.3	FIA_PSK_EXT.1/MACsec Guidance 2.....	80
5.6.4	FIA_PSK_EXT.1/VPN .....	81
5.6.4.1	FIA_PSK_EXT.1/VPN TSS 1 .....	81
5.6.4.2	FIA_PSK_EXT.1/VPN Guidance 1.....	81
5.6.4.3	FIA_PSK_EXT.1/VPN Guidance 2.....	82
5.6.5	FIA_UIA_EXT.1.....	83
5.6.5.1	FIA_UIA_EXT.1 TSS 1 .....	83
5.6.5.2	FIA_UIA_EXT.1 TSS 2 .....	84
5.6.5.3	FIA_UIA_EXT.1 Guidance 1 .....	84
5.6.6	FIA_UAU.7 .....	85
5.6.6.1	FIA_UAU.7 Guidance 1.....	85
5.6.7	FIA_X509_EXT.1/Rev.....	85
5.6.7.1	FIA_X509_EXT.1/Rev TSS 1 .....	85
5.6.7.2	FIA_X509_EXT.1/Rev TSS 2 .....	86
5.6.7.3	FIA_X509_EXT.1/Rev Guidance 1.....	86
5.6.8	FIA_X509_EXT.2 .....	87
5.6.8.1	FIA_X509_EXT.2 TSS 1.....	87
5.6.8.2	FIA_X509_EXT.2 TSS 2.....	88
5.6.8.3	FIA_X509_EXT.2 Guidance 1 .....	89
5.6.8.4	FIA_X509_EXT.2 Guidance 2 .....	89
5.6.8.5	FIA_X509_EXT.2 Guidance 3 .....	90
5.6.9	FIA_X509_EXT.3 .....	90
5.6.9.1	FIA_X509_EXT.3 TSS 1.....	90

5.6.9.2	FIA_X509_EXT.3 Guidance 1 .....	91
<b>5.7</b>	<b>TSS and Guidance Activities (Security Management) .....</b>	<b>91</b>
5.7.1	FMT_MOF.1/ManualUpdate.....	91
5.7.1.1	FMT_MOF.1/ManualUpdate Guidance 1 .....	91
5.7.2	FMT_FMT_MOF.1/Functions .....	92
5.7.2.1	FMT_MOF.1/Functions TSS 2.....	92
5.7.2.2	FMT_MOF.1/Functions Guidance 2 .....	92
5.7.3	FMT_MOF.1/Services.....	93
5.7.3.1	FMT_MOF.1/Services TSS 2 .....	93
5.7.3.2	FMT_MOF.1/Services Guidance 2.....	93
5.7.4	FMT_MTD.1/CoreData.....	93
5.7.4.1	FMT_MTD.1/CoreData TSS 1 .....	93
5.7.4.2	FMT_MTD.1/CoreData TSS 2 .....	94
5.7.4.3	FMT_MTD.1/CoreData Guidance 1 .....	95
5.7.4.4	FMT_MTD.1/CoreData Guidance 2 .....	95
5.7.5	FMT_MTD.1/CryptoKeys.....	96
5.7.5.1	FMT_MTD.1/CryptoKeys TSS 2 .....	96
5.7.5.2	FMT_MTD.1/CryptoKeys Guidance 2 .....	97
5.7.6	FMT_SMF.1 .....	98
5.7.6.1	FMT_SMF.1 TSS 1.....	98
5.7.6.2	FMT_SMF.1 TSS 2.....	100
5.7.6.3	FMT_SMF.1 Guidance 1 .....	101
5.7.1	FMT_SMF.1/VPN.....	102
5.7.1.1	FMT_SMF.1/VPN TSS .....	102
5.7.1.2	FMT_SMF.1/VPN Guidance .....	103
5.7.1.3	FMT_SM .....	<b>Error! Bookmark not defined.</b>
5.7.1.4	FMT_SMF.1 Guidance 1 .....	103
5.7.2	FMT_SMR.2 .....	104
5.7.2.1	FMT_SMR.2 TSS 1 .....	104
5.7.2.2	FMT_SMR.2 Guidance 1.....	104
<b>5.8</b>	<b>TSS and Guidance Activities (Packet Filtering) .....</b>	<b>105</b>
5.8.1	FPF_RUL_EXT.1 .....	105
5.8.1.1	FPF_RUL_EXT.1.1 TSS 1 .....	105
5.8.1.2	FPF_RUL_EXT.1.1 Guidance 1 .....	106
5.8.1.3	FPF_RUL_EXT.1.4 TSS 1.....	106
5.8.1.4	FPF_RUL_EXT.1.4 Guidance 1 .....	108
5.8.1.5	FPF_RUL_EXT.1.5 TSS 1 .....	110
5.8.1.6	FPF_RUL_EXT.1.5 Guidance 1 .....	111
5.8.1.7	FPF_RUL_EXT.1.6 TSS 1 [TD0597].....	111
5.8.1.8	FPF_RUL_EXT.1.6 Guidance 1 [TD0597] .....	113
<b>5.9</b>	<b>TSS and Guidance Activities (Protection of the TSF) .....</b>	<b>114</b>
5.9.1	FPT_APW_EXT.1.....	114
5.9.1.1	FPT_APW_EXT.1 TSS 1 .....	114
5.9.2	FPT_SKP_EXT.1.....	115
5.9.2.1	FPT_SKP_EXT.1 TSS 1 .....	115
5.9.3	FPT_STM_EXT.1.....	115
5.9.3.1	FPT_STM_EXT.1 TSS 1 [TD0632].....	115
5.9.3.2	FPT_STM_EXT.1 Guidance 1 .....	116



5.9.4	FPT_TST_EXT.1.1 .....	116
5.9.4.1	FPT_TST_EXT.1.1 TSS 1 .....	116
5.9.4.2	FPT_TST_EXT.1.1 Guidance 1 .....	117
5.9.5	FPT_TST_EXT.3 .....	118
5.9.5.1	FPT_TST_EXT.3 TSS .....	118
5.9.6	FPT_TUD_EXT.1 .....	118
5.9.6.1	FPT_TUD_EXT.1 TSS 1 .....	118
5.9.6.2	FPT_TUD_EXT.1 TSS 2 .....	119
5.9.6.3	FPT_TUD_EXT.1 TSS 3 .....	119
5.9.6.4	FPT_TUD_EXT.1 TSS 5 .....	120
5.9.6.5	FPT_TUD_EXT.1 Guidance 1 .....	120
5.9.6.6	FPT_TUD_EXT.1 Guidance 2 .....	121
5.9.6.7	FPT_TUD_EXT.1 Guidance 3 .....	122
5.9.6.8	FPT_TUD_EXT.1 Guidance 6 .....	122
<b>5.10</b>	<b>TSS and Guidance Activities (TOE Access) .....</b>	<b>122</b>
5.10.1	FTA_SSL_EXT.1 .....	122
5.10.1.1	FTA_SSL_EXT.1 TSS 1 .....	122
5.10.1.2	FTA_SSL_EXT.1 Guidance 1 .....	123
5.10.2	FTA_SSL.3 .....	124
5.10.2.1	FTA_SSL.3 TSS 1 .....	124
5.10.2.2	FTA_SSL.3 Guidance 1 .....	124
5.10.3	FTA_SSL.4 .....	125
5.10.3.1	FTA_SSL.4 TSS 1 .....	125
5.10.3.2	FTA_SSL.4 Guidance 1 .....	125
5.10.4	FTA_TAB.1 .....	125
5.10.4.1	FTA_TAB.1 TSS 1 .....	125
5.10.4.2	FTA_TAB.1 Guidance 1 .....	126
<b>5.11</b>	<b>TSS and Guidance Activities (Trusted Path/Channels) .....</b>	<b>126</b>
5.11.1	FTP_ITC.1 .....	126
5.11.1.1	FTP_ITC.1 TSS 1 .....	126
5.11.1.2	FTP_ITC.1 Guidance 1 .....	127
5.11.2	FTP_ITC.1/VPN .....	128
5.11.2.1	FTP_ITC.1/VPN TSS 1 .....	128
5.11.2.2	FTP_ITC.1/VPN Guidance .....	129
5.11.3	FTP_TRP.1/Admin .....	129
5.11.3.1	FTP_TRP.1/Admin TSS 1 .....	129
5.11.3.2	FTP_TRP.1/Admin Guidance 1 .....	130
<b>6</b>	<b>Detailed Test Cases (Test Activities) .....</b>	<b>131</b>
6.1	FAU_GEN.1 Test #1 .....	131
6.1	FAU_STG_EXT.1 Test #1 .....	131
6.2	FAU_STG_EXT.1 Test #2 (b) .....	132
6.3	FPT_STM_EXT.1 Test #1 .....	132
6.4	FTP_ITC.1 Test #1 .....	133
6.5	FTP_ITC.1 Test #2 .....	133
6.6	FTP_ITC.1 Test #3 .....	133
6.7	FTP_ITC.1 Test #4 .....	133
6.8	FCS_CKM.2 Test #2 .....	134

6.9	FIA_AFL.1 Test #1.....	135
6.10	FIA_AFL.1 Test #2a.....	135
6.11	FIA_PMG_EXT.1 Test #1 .....	136
6.12	FIA_PMG_EXT.1 Test #2 .....	136
6.13	FIA_UIA_EXT.1 Test #1 .....	137
6.14	FIA_UIA_EXT.1 Test #2 .....	138
6.15	FIA_UIA_EXT.1 Test #3 .....	138
6.16	FIA_UAU.7 Test #1 .....	139
6.17	FMT_MOF.1/ManualUpdate Test #1 .....	139
6.18	FMT_MOF.1/ManualUpdate Test #2 .....	139
6.19	FMT_MOF.1/Functions (1) Test #1 .....	140
6.20	FMT_MOF.1/Functions (1)Test #2 .....	140
6.21	FMT_MOF.1/Services Test #1.....	141
6.22	FMT_MOF.1/Services Test #2.....	141
6.23	FMT_MTD.1/CryptoKeys Test #1.....	141
6.24	FMT_MTD.1/CryptoKeys Test #2.....	142
6.25	FMT_SMF.1 Test #1.....	142
6.26	FMT_SMR.2 Test #1 .....	143
6.27	FTA_SSL.3 Test #1 .....	143
6.28	FTA_SSL.4 Test #1 .....	143
6.29	FTA_SSL.4 Test #2 .....	144
6.30	FTA_SSL_EXT.1.1 Test #1.....	144
6.31	FTA_TAB.1 Test #1 .....	145
6.32	FTP_TRP.1/Admin Test #1 .....	145
6.33	FTP_TRP.1/Admin Test #2 .....	146
6.34	FCS_SSHS_EXT.1.2 Test #1.....	146
6.35	FCS_SSHS_EXT.1.2 Test #2.....	146
6.36	FCS_SSHS_EXT.1.2 Test #3.....	147
6.37	FCS_SSHS_EXT.1.2 Test #4.....	147
6.38	FCS_SSHS_EXT.1.3 Test #1.....	148
6.39	FCS_SSHS_EXT.1.4 Test #1.....	148
6.40	FCS_SSHS_EXT.1.5 Test #1.....	149
6.41	FCS_SSHS_EXT.1.5 Test #2.....	149
6.42	FCS_SSHS_EXT.1.6 Test #1.....	150
6.43	FCS_SSHS_EXT.1.6 Test #2.....	150
6.44	FCS_SSHS_EXT.1.7 Test #1.....	151
6.45	FCS_SSHS_EXT.1.7 Test #2.....	151
6.46	FCS_SSHS_EXT.1.8 Test #1t .....	151
6.47	FCS_SSHS_EXT.1.8 Test #1b.....	152
6.48	FCS_IPSEC_EXT.1.1 Test #1.....	153
6.49	FCS_IPSEC_EXT.1.1 Test #2.....	154
6.50	FCS_IPSEC_EXT.1.2 Test #1.....	155
6.51	FCS_IPSEC_EXT.1.3 Test #1.....	156
6.52	FCS_IPSEC_EXT.1.3 Test #2.....	156
6.53	FCS_IPSEC_EXT.1.4 Test #1.....	157

6.54	FCS_IPSEC_EXT.1.5 Test #1	158
6.55	FCS_IPSEC_EXT.1.5 Test #2	158
6.56	FCS_IPSEC_EXT.1.6 Test #1	159
6.57	FCS_IPSEC_EXT.1.7 Test #1	161
6.58	FCS_IPSEC_EXT.1.7 Test #2	161
6.59	FCS_IPSEC_EXT.1.8 Test #1	162
6.60	FCS_IPSEC_EXT.1.8 Test #2	162
6.61	FCS_IPSEC_EXT.1.10 Test #1	163
6.62	FCS_IPSEC_EXT.1.10 Test #2	164
6.63	FCS_IPSEC_EXT.1.11 Test #1	164
6.64	FCS_IPSEC_EXT.1.12 Test #1	165
6.65	FCS_IPSEC_EXT.1.12 Test #2	166
6.66	FCS_IPSEC_EXT.1.12 Test #3	166
6.67	FCS_IPSEC_EXT.1.12 Test #4	167
6.68	FCS_IPSEC_EXT.1.14 Test #1	167
6.69	FCS_IPSEC_EXT.1.14 Test #3	168
6.70	FCS_IPSEC_EXT.1.14 Test #5	169
6.71	FCS_IPSEC_EXT.1.14 Test #6a	169
6.72	FCS_IPSEC_EXT.1.14 Test #6b	170
6.73	FIA_X509_EXT.1.1/Rev Test #1a	171
6.74	FIA_X509_EXT.1.1/Rev Test #1a(ECDSA)	171
6.75	FIA_X509_EXT.1.1/Rev Test #1b	172
6.76	FIA_X509_EXT.1.1/Rev Test #2	172
6.77	FIA_X509_EXT.1.1/Rev Test #3(CRL)	173
6.78	FIA_X509_EXT.1.1/Rev Test #4(CRL)	174
6.79	FIA_X509_EXT.1.1/Rev Test #5	174
6.80	FIA_X509_EXT.1.1/Rev Test #6	175
6.81	FIA_X509_EXT.1.1/Rev Test #7	175
6.82	FIA_X509_EXT.1.1/Rev Test #8a	176
6.83	FIA_X509_EXT.1.1/Rev Test #8b	176
6.84	FIA_X509_EXT.1.1/Rev Test #8c	177
6.85	FIA_X509_EXT.1.2/Rev Test #1	177
6.86	FIA_X509_EXT.1.2/Rev Test #2	178
6.87	FIA_X509_EXT.2 Test #1(CRL)	179
6.88	FIA_X509_EXT.3 Test #1	179
6.89	FIA_X509_EXT.3 Test #2	180
6.90	FPT_TST_EXT.1 Test #1	180
6.91	FPT_TUD_EXT.1 Test #1	181
6.92	FPT_TUD_EXT.1 Test #2 (a)	181
6.93	FPT_TUD_EXT.1 Test #2 (b)	182
6.94	FPT_TUD_EXT.1 Test #2 (c)	182
6.95	PSK_EXT.1 Test #2	183
6.96	FIA_PSK_EXT.1 Test #3	183
6.97	FIA_PSK_EXT.1 Test #4	184
6.98	FAU_GEN.1/VPN Test #1(MOD_VPNGW)	184

6.99 FAU_GEN.1/VPN Test #2 (MOD_VPNGW).....	184
6.100 FMT_SMF.1 Test #1(MOD_VPNGW) .....	185
6.101 FPF_RUL_EXT.1.1 Test #1 .....	185
6.102 FPF_RUL_EXT.1.1 Test #2 .....	186
6.103 FPF_RUL_EXT.1.4 Test #1 .....	186
6.104 FPF_RUL_EXT.1.4 Test #2 .....	187
6.105 FPF_RUL_EXT.1.5 Test #1 .....	188
6.106 FPF_RUL_EXT.1.5 Test #2 .....	188
6.107 FPF_RUL_EXT.1.6 Test #1 .....	189
6.108 FPF_RUL_EXT.1.6 Test #2 .....	190
6.109 FPF_RUL_EXT.1.6 Test #3 .....	192
6.110 FPF_RUL_EXT.1.6 Test #4 .....	193
6.111 FPF_RUL_EXT.1.6 Test #5 .....	194
6.112 FPF_RUL_EXT.1.6 Test #6 .....	196
6.113 FPF_RUL_EXT.1.6 Test #7 .....	197
6.114 FPF_RUL_EXT.1.6 Test #8 .....	198
6.115 FPF_RUL_EXT.1.6 Test #9 .....	199
6.116 FPF_RUL_EXT.1.6 Test #10 .....	199
6.117 FAU_GEN.1/MACSEC Test #1.....	200
6.118 FCS_MACSEC_EXT.1 Test #1 .....	200
6.119 FCS_MACSEC_EXT.1 Test #2 .....	201
6.120 FCS_MACSEC_EXT.2 Test #1 .....	201
6.121 FCS_MACSEC_EXT.2 Test #2 .....	202
6.122 FCS_MACSEC_EXT.4 Test #1 .....	202
6.123 FCS_MACSEC_EXT.4 Test #2 .....	203
6.124 FCS_MKA_EXT.1.2 Test #1.....	203
6.125 FCS_MKA_EXT.1.4 Test #1.....	203
6.126 FCS_MKA_EXT.1.4 Test #2.....	204
6.127 FCS_MKA_EXT.1.5 Test #1.....	204
6.128 FCS_MKA_EXT.1.5 Test #2.....	205
6.129 FCS_MKA_EXT.1.8 Test #1.....	205
6.130 FCS_MKA_EXT.1.8 Test #2a.....	206
6.131 FCS_MKA_EXT.1.8 Test #2b.....	206
6.132 FCS_MKA_EXT.1.8 Test #2c .....	207
6.133 FCS_MKA_EXT.1.8 Test #2d.....	207
6.134 FCS_MKA_EXT.1.8 Test #2e.....	208
6.135 FIA_AFL.1 Test #1 (MACsec) .....	208
6.136 FIA_AFL.1 Test #2 (MACsec) .....	208
6.137 FIA_PSK_EXT.1/MACSEC Test #1 .....	209
6.138 FIA_PSK_EXT.1/MACSEC Test #2 .....	209
6.139 FIA_PSK_EXT.1/MACSEC Test #3 .....	210
6.140 FMT_SMF.1/MACSEC Test #1 .....	210
6.141 FMT_SMF.1/MACSEC Test #2 .....	211
6.142 FMT_SMF.1/MACSEC Test #3a .....	211
6.143 FMT_SMF.1/MACSEC Test #3b .....	212

6.144	FMT_SMF.1/MACSEC Test #4 .....	213
6.145	FPT_FLS.1(2)/SelfTest Test #1.....	213
6.146	FPT_RPL.1 Test #1 .....	214
6.147	FPT_RPL.1 Test #2 .....	214
6.148	FTP_ITC.1/MACSEC Test #1 .....	214
6.149	FTP_TRP.1/MACSEC Test #1 .....	215
<b>7</b>	<b>Security Assurance Requirements.....</b>	<b>216</b>
7.1	ADV_FSP.1 Basic Functional Specification.....	216
7.1.1	ADV_FSP.1.....	216
7.1.1.1	ADV_FSP.1 Activity 1.....	216
7.1.1.2	ADV_FSP.1 Activity 2.....	216
7.1.1.3	ADV_FSP.1 Activity 3.....	216
7.2	AGD_OPE.1 Operational User Guidance .....	216
7.2.1	AGD_OPE.1.....	216
7.2.1.1	AGD_OPE.1 Activity 1.....	216
7.2.1.2	AGD_OPE.1 Activity 2.....	217
7.2.1.3	AGD_OPE.1 Activity 3.....	217
7.2.1.4	AGD_OPE.1 Activity 4.....	218
7.2.1.5	AGD_OPE.1 Activity 5 [TD0536] .....	218
7.3	AGD_PRE.1 Preparative Procedures .....	218
7.3.1	AGD_PRE.1 .....	218
7.3.1.1	AGD_PRE.1 Activity 1 .....	218
7.3.1.2	AGD_PRE.1 Activity 2 .....	219
7.3.1.3	AGD_PRE.1 Activity 3 .....	220
7.3.1.4	AGD_PRE.1 Activity 4 .....	221
7.3.1.5	AGD_PRE.1 Activity 5 .....	221
7.4	ALC Assurance Activities .....	221
7.4.1	ALC_CMC.1.....	221
7.4.1.1	ALC_CMC.1 Activity 1.....	221
7.4.2	ALC_CMS.1 .....	222
7.4.2.1	ALC_CMS.1 Activity 1 .....	222
7.5	ATE_IND.1 Independent Testing – Conformance.....	222
7.5.1	ATE_IND.1 .....	222
7.5.1.1	ATE_IND.1 Activity 1 .....	222
7.6	AVA_VAN.1 Vulnerability Survey .....	222
7.6.1	AVA_VAN.1.....	222
7.6.1.1	AVA_VAN.1 Activity 1 [TD0564].....	222
7.6.1.2	AVA_VAN.1 Activity 2 .....	224
7.6.1.3	AVA_VAN.1/VPN Activity 1 .....	225
<b>8</b>	<b>Conclusion.....</b>	<b>226</b>

# 1 TOE Overview

## 1.1 TOE Description

This section provides an overview of the Cat8200 and Cat8500 Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the Cat8200 and Cat8500 routers. The TOE software for each platform is comprised of Cisco IOS-XE version 17.6. The Cisco IOS-XE version 17.6 software is used to meet all of the requirements as specified in this document regardless of the hardware platform.

### 1.1.1 Cisco Catalyst 8200 Series Edge Routers (Cat8200)

This section defines the Cat8200 components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The software is comprised of Cisco IOS-XE version 17.6. The hardware models included in the evaluation are: C8200-1N-4T, C8200L-1N-4T with MACsec network interface module (NIM): C-NIM-2T.

The TOE consists of a number of components including:

- Chassis: The TOE chassis is a 1-RU form factor.
- Integrated Gigabit Ethernet ports:
  - Provides four built-in Ethernet WAN ports
  - Two Ethernet ports in Small Form-Factor Pluggable (SFP) and two RJ45 ports
- DRAM: 8GB (C8200-1N-4T), 4GB (C8200L-1N-4T). Both platforms can be upgraded to 16GB or 32GB.
- Flash memory: integrated on-board 8GB
- Cisco Network Interface Modules (NIM): One integrated NIM slot allows for flexible configurations.

### 1.1.2 Cisco Catalyst 8500 Series Edge Routers (Cat8500)

This section defines the Cat8500 components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The software is comprised of Cisco IOS-XE version 17.6. The hardware models included in the evaluation are: C8500L-8S4X.

The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 1-RU form factor.
- Integrated Gigabit Ethernet ports:
  - Four 1/10GE
  - Eight 1GE ports
- Flash storage: 32GB
- DRAM: The default is 16GB and can be upgraded to 32GB or 64GB.

## 2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPPv2.2e, the MOD\_VPNGW\_v1.1 and the PP\_NDCPP\_MACSEC\_EP\_V1.2 based upon the core SFRs and those implemented based on selections within the PPs/EPs.

### 3 Test Equivalency Justification

The Cisco Catalyst 8200 and 8500 Series Edge Routers (herein after referred to as the Cat8200 and Cat8500 respectively) are purpose-built, routing platforms that includes VPN functionality and MACsec encryption provided by the Cisco IOS-XE software. The TOE is a hardware and software solution that makes up the router models as follows:

- Cat8200
  - C8200-1N-4T
  - C8200L-1N-4T
- Cat8500
  - C8500L-8S4X

For Cat8500, only one mode is claimed for the evaluation and full testing will be done on C8500L-8S4X. Therefore, no equivalency analysis is required for Cat8500.

This section provides a testing equivalency analysis for the Cisco Catalyst 8200/8200L Series Edge Routers running IOS-XE 17.6. This analysis provides an explanation of the differences between each of the hardware models included within the TOE boundary and provides an analysis of the impact each of the differences have on the TSF functionality

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPPv2.2e. Additionally, a comparison of the data presented in section 3 is provided to identify a testing subset that will exercise each of the differences in TOE models.

#### 3.1 OS, Processor, and Firmware Analysis

The following table compares the Operating System, CPU, and firmware that runs on each of the included TOE platforms.

**Table 1 – Image Analysis**

TOE Model	Image	Analysis
C8200-1N-4T	Cisco IOS-XE 17.6	TOE is the Cisco Catalyst 8200/8200L Series Edge Routers all run identical IOS-XE version 17.6.  VERDICT: The Catalyst 8200 & 8200L Series Edge routers share the IOS module version IOS-XE 17.6
C8200L-1N-4T	Cisco IOS-XE 17.6	

**Table 2 – Processor Analysis**

TOE	Processor	Analysis
C8200-1N-4T	Intel Xeon D-1563N (Broadwell) C-NIM-2T MACsec - Broadcom BCM54194	C8200-1N-4Tseries edge router uses Intel Xeon D-1563N (Broadwell). Xeon D-1563N is a 64-bit Octa core x86 micro server single-chip processors The D-1563N is based on the Broadwell microarchitecture and is fabricated on their 14 nm processor.






TOE	Processor	Analysis
C8200L-1N-4T	Intel Xeon D-1573N (Broadwell) C-NIM-2T MACsec - Broadcom BCM54194	C8200L-1N-4Tseries edge router uses Intel Xeon D-1573N (Broadwell). Xeon D-1573N is a 64-bit Octa core x86microserver single-chip processors The D-1573N is based on the Broadwell microarchitecture and is fabricated on their 14 nm processor.

### 3.2 Specification of Differences

The following tables provide a description of the physical differences between hardware models

**Table 3 Hardware Models and Specifications**

Hardware Model	Processor/MACSEC PHY	Size Physical dimensions (H x W x D in.)	Interfaces
C8200-1N-4T C8200L-1N-4T 	C8200-1N-4T <ul style="list-style-type: none"> <li>Intel Xeon D-1563N (Broadwell)</li> </ul> C-NIM-2T <ul style="list-style-type: none"> <li>MACsec - Broadcom BCM54194</li> </ul>	<ul style="list-style-type: none"> <li>1.71 x 17.3 x 16.5 RU</li> </ul>	<b>Interfaces</b> C8200-1N-4T <ul style="list-style-type: none"> <li>1 NIM Slot</li> <li>4x 1-Gigabit Ethernet Ports (2x SFP, 2x RJ45)</li> </ul> C-NIM-2T <ul style="list-style-type: none"> <li>2x 1-Gigabit Ethernet Ports</li> </ul>
C8200L-1N-4T 	C8200L-1N-4T <ul style="list-style-type: none"> <li>Intel Xeon D-1573N (Broadwell)</li> </ul> C-NIM-2T <ul style="list-style-type: none"> <li>MACsec - Broadcom BCM54194</li> </ul>	<ul style="list-style-type: none"> <li>1.71 x 17.3 x 16.5 RU</li> </ul>	C8200L-1N-4T <ul style="list-style-type: none"> <li>1 NIM Slot</li> <li>4x 1-Gigabit Ethernet Ports (2x SFP, 2x RJ45)</li> </ul> C-NIM-2T <ul style="list-style-type: none"> <li>2x 1-Gigabit Ethernet Ports</li> </ul>
C8500L-8S4X 	<ul style="list-style-type: none"> <li>Intel Xeon D-2168NT (Skylake)</li> <li>MACsec - Broadcom BCM82757/BCM54194</li> </ul>	<ul style="list-style-type: none"> <li>1.73 x 17.50 x 18.46 1RU</li> </ul>	<b>Interfaces</b> <ul style="list-style-type: none"> <li>4x 1/10GE ports</li> <li>8x 1GE ports</li> </ul>

### 3.3 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF functionality. The hardware within the TOE only differs by configuration and performance. Except for the MACsec encryption hardware, and hardware entropy sources, there are no hardware specific dependencies of the product.

The ASIC used to perform MACsec encryption is the same across all models. The hardware models within the TOE have common hardware characteristics. These characteristics affect only non-TOE Security Function (TSF)

relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

There is one hardware entropy source that seeds the software DRBG implemented within Platform Independent IOS-XE software. Because of this a single entropy analysis was performed.

TOE uses Intel® Quick Assist Technology (QAT) to give hardware acceleration to VPN encryption & decryption operations.

There is a two MACsec co-processor, therefore MACsec testing can be performed on a single device.

Result: Single entropy analysis and single device testing for MACsec.

### **3.4 Software/OS Dependencies:**

This category of differences is only applicable if the TOE is installed on an OS outside of the TOE boundary. In this case, all software including the OS is included in IOS-XE and within the TOE boundary. There are no specific dependencies on the OS since the TOE will not be installed on different OSs. The image used on Catalyst 8200 and 8200L series models is comprised of the Universal Cisco IOS-XE 17.6. The image used on each platform is identical.

Result: All platforms are equivalent.

### **3.5 Differences in Libraries Used to Provide TOE Functionality**

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. Of note, the TOE uses the same cryptographic module to provide its cryptographic functionality. This is the same across platforms.

Result: All platforms are equivalent.

### **3.6 TOE Management Interface Differences**

The TOE is managed via either remote CLI session or directly connected CLI. These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

Result: All platforms are equivalent

### **3.7 TOE Functional Differences**

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available to the user in for each of these devices. Each device runs the same version of IOS-XE software. For IOS-XE/IOS software, differences in the provided functionality is denoted by a different version of the software. If there had been differences in the functionality provided by the software, the actual release version would have been different for the platform.

Result: All platforms are equivalent.

### **3.8 MACsec Analysis**

The evaluation team reviewed the ST and examined the TOE hardware models including an ASIC used for MACsec. All TOE models utilize the same ASIC for MACsec functionality. The ASIC used for MACsec has a CAVP certificate (4544 ,4550) for AES.

### **3.9 Difference Comparison**

All platforms run the same software and perform identical functionality. All platforms use identical processors for MACsec operation. The only security relevant difference for each platform is the base CPU. Each family of platform includes a separate processor.

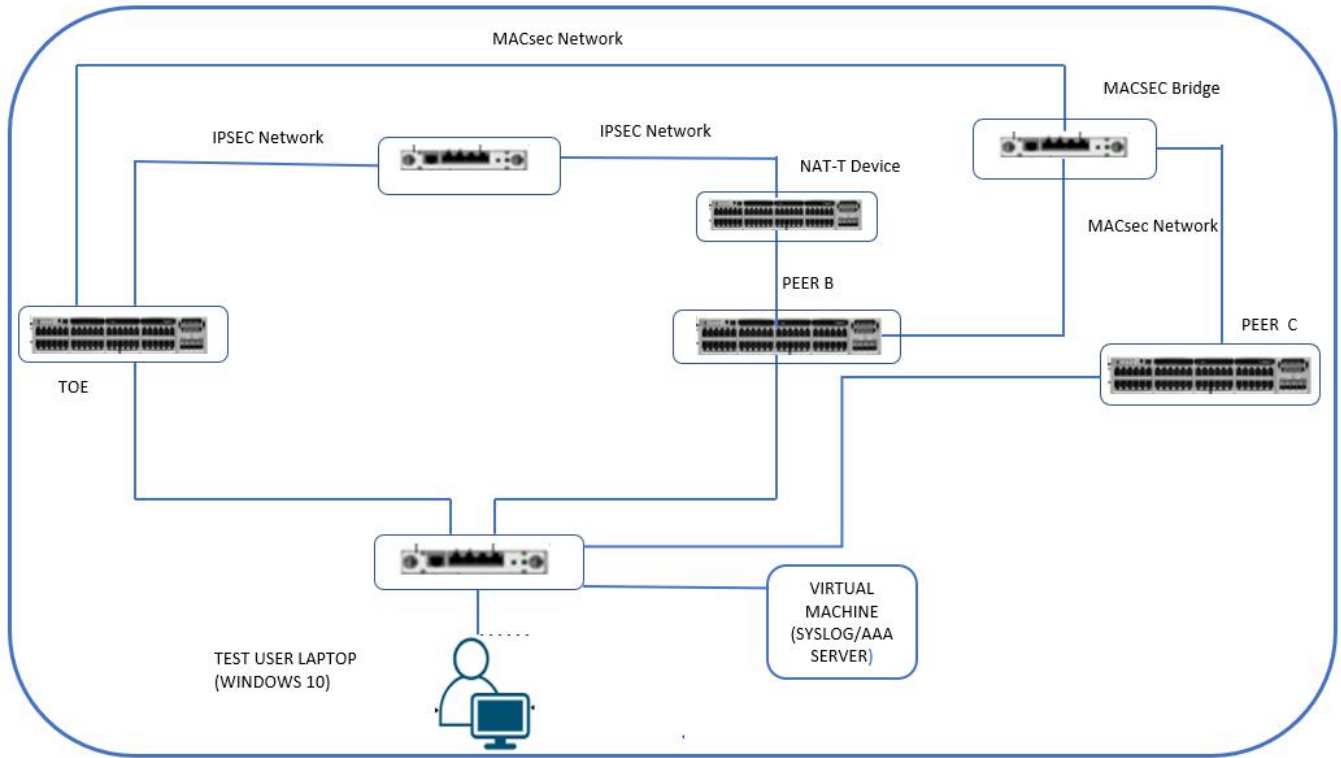
### 3.10 Recommendations/Conclusions

Based on the equivalency rationale listed above, testing will be performed on the following subset,

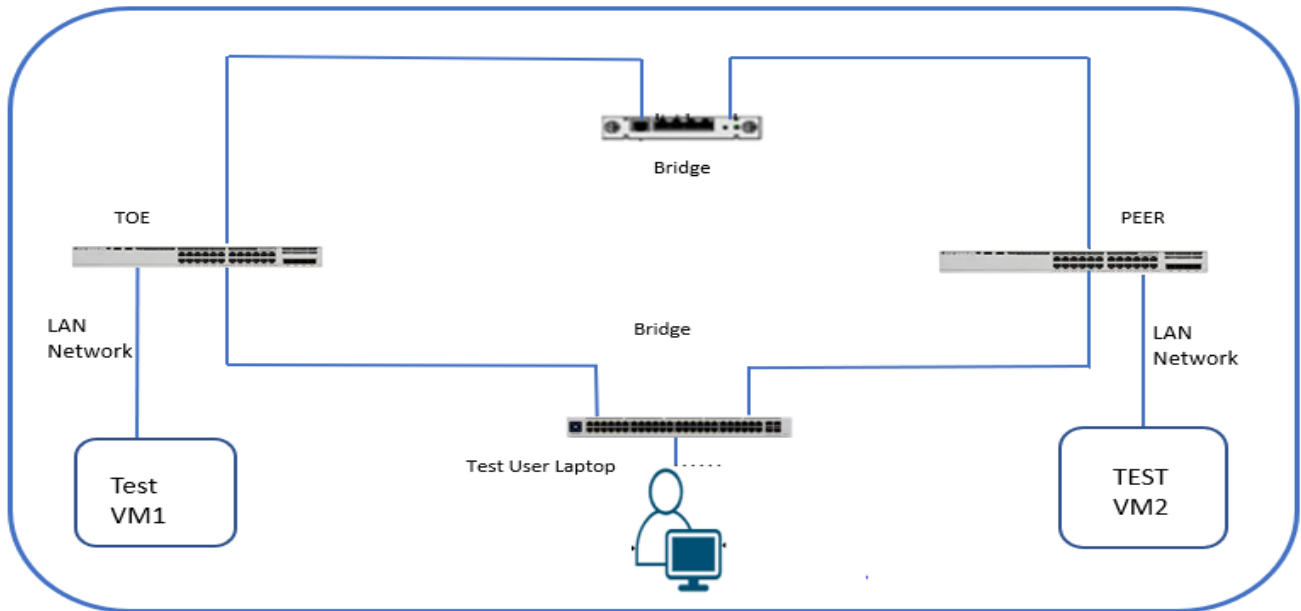
- NDcPP Testing:
  - 1 example from either of the families
- MACsec Testing:
  - 1 example from either of the families
- VPNGW testing
  - 1 example from either of the families

# 4 Test Bed Descriptions

## NDcPP + MACsec



## VPN



## 4.1 Test Bed Details

Name	OS	Function	Protocols	Time	Tools (version)
TOE (C8200-1N-4T/ C8200L-1N-4T)	IOS XE 17.6.1a	TOE	SSH, IPsec, MACsec	Manually set and verified	
Peer B (C8500L-8S4X)	IOS XE 17.6.1a	Peer	SSH, IPsec, MACsec	Manually set and verified	
Peer C(ASR1001-HX)	IOS-XE 17.03.01a	Peer	MACsec	Manually set and verified	
Cisco C1131	Cisco IOS-XE version 17.9	NAT-T Device		Manually set and verified	
IPsec Bridge	Ubuntu 18.04.6 LTS	Packet Capture	N/A	Manually set and verified	tcpdump version (4.9.3) libpcap version (1.8.1)
Bridge /TestVM1	Linux kali 5.9.0-kali1- amd64	Packet Capture/ Radius Server/ Syslog Server/ CRL Server/ CA server/ Managemen t Workstation	SSH,CRL, RADIUS, Syslog, CA	Manually set and verified	tcpdump version (4.99.1) libpcap version (1.10.1) OpenSSL (1.1.1m) FreeRADIUS Version (3.0.21) rsyslogd version (8.2208.0) StrongSwan Version (5.9.2)
MACsec Bridge	Ubuntu 20.04.4 LTS	Packet Capture		Manually set and verified	tcpdump version (4.9.3) libpcap version (1.9.1)
Test VM2	Ubuntu 20.04.4 LTS	Packet Capture		Manually set and verified	tcpdump version (4.9.3) libpcap version (1.8.1) OpenSSL (1.1.1)
Test user Laptop	Windows 10 pro	Test workstation/ Managemen t Workstation	SSH	Manually set and verified	PuTTY 0.76, XCA 2.1.1, WinSCP 5.19.3 Wireshark 3.6.1

## **4.2 Test Time & Location**

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from February 2021 to January 2023.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

## 5 Detailed Test Cases (TSS and Guidance Activities)

### 5.1 TSS and Guidance Activities (Auditing)

#### 5.1.1 FAU\_GEN.1

##### 5.1.1.1 FAU\_GEN.1 TSS 1

Objective	For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.
Evaluator Findings	<p>The evaluator examined the <b>FAU_GEN.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys:</p> <p><b>The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, “Auditable Events Table”). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key and a key reference. Additionally, the startup and shutdown of the audit functionality is audited.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### 5.1.1.2 FAU\_GEN.1 TSS 3 (VPNGWMod)

Objective	The evaluator shall verify that the TSS describes how the TSF can be configured to log network traffic associated with applicable rules. Note that this activity may be addressed in conjunction with the TSS Evaluation Activities for FPF_RUL_EXT.1.
Evaluator Findings	<p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how the TSF can be configured to log network traffic associated with applicable rules. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using access and crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. The access lists can be applied to all the network interfaces.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### 5.1.1.3 FAU\_GEN.1 TSS 4 (VPNGWMod)

Objective	The evaluator shall verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. It is acceptable for the TOE to drop packets that
-----------	---

	it cannot process, but under no circumstances is the TOE allowed to pass packets that do not satisfy a rule that allows the permit operation or belong to an allowed established session. It may not always be possible for the TOE to audit dropped packets due to implementation limitations. These limitations and circumstances in which the event of dropped packets is not audited shall be described in the TSS.
Evaluator Findings	<p>The evaluator examined the <b>FAU_GEN.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>When the incoming traffic to the TOE exceeds what the interface can handle, the packets are dropped at the input queue itself and there are no error messages generated.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.1.1.4 FAU\_GEN.1 TSS 5 (VPNGWMod)

Objective	The evaluator also verifies that the TSS describes the auditable events for IPsec peer session establishment that are required by the PP-Module.
Evaluator Findings	<p>The evaluator examined the <b>FAU_GEN.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the auditable events for IPsec peer session establishment that are required by the PP-Module. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE generates an audit record whenever any of the audited events in Table 14 occurs. The types of events that cause audit records to be generated include startup and shutdown of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key. Additionally, the startup and shutdown of the audit functionality is audited.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.1.1.5 FAU\_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	The evaluator examined the section titled <b>Security Relevant Events</b> in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the that the tables ' <b>Table 6 General Auditable Events</b> ' and ' <b>Table 7 Auditable Administrative Events</b> ' in the AGD contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2, as



	<p>well as an example audit record. The evaluator next compared this list of events to the auditable events listed in the NDcPP.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1.6 FAU\_GEN.1 Guidance 2

Objective	<p>The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.</p>																																			
Evaluator Findings	<p>The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:</p> <table border="1"> <thead> <tr> <th>Administrative Activity</th> <th>Method (Command/GUI Configuration)</th> <th>Section</th> </tr> </thead> <tbody> <tr> <td>Startup/shutdown of the Audit Function</td> <td>A series of CLI commands is provided for configuration</td> <td>Section 3.3.3</td> </tr> <tr> <td>Terminating session</td> <td>Exit Logout</td> <td>Section 3.3.1</td> </tr> <tr> <td>Display system information</td> <td>show version</td> <td>Section 2 - Step 11</td> </tr> <tr> <td>Login Banner</td> <td>banner login d This is a banner d</td> <td>Section 4.5</td> </tr> <tr> <td>Session Termination</td> <td>exec-timeout &lt;time&gt;</td> <td>Section 3.2.5</td> </tr> <tr> <td>Lockout configuration</td> <td>aaa local authentication attempts max-fail [<i>number of failures</i>]</td> <td>Section 3.2.6</td> </tr> <tr> <td>Setting Password Length</td> <td>security passwords min-length <i>length</i></td> <td>Section 4.2</td> </tr> <tr> <td>Creating Users</td> <td>username &lt;name&gt; password &lt;password&gt;</td> <td>Section 3.2.4</td> </tr> <tr> <td>Management of Crypto Keys</td> <td>crypto key generate rsa modulus 3072  crypto key generate ec keysize &lt;256   384&gt; exportable</td> <td>Section 4.6.4.1</td> </tr> <tr> <td>Clock Management</td> <td>A series of CLI commands are provided for configuration</td> <td>Section 4.3</td> </tr> </tbody> </table>			Administrative Activity	Method (Command/GUI Configuration)	Section	Startup/shutdown of the Audit Function	A series of CLI commands is provided for configuration	Section 3.3.3	Terminating session	Exit Logout	Section 3.3.1	Display system information	show version	Section 2 - Step 11	Login Banner	banner login d This is a banner d	Section 4.5	Session Termination	exec-timeout <time>	Section 3.2.5	Lockout configuration	aaa local authentication attempts max-fail [ <i>number of failures</i> ]	Section 3.2.6	Setting Password Length	security passwords min-length <i>length</i>	Section 4.2	Creating Users	username <name> password <password>	Section 3.2.4	Management of Crypto Keys	crypto key generate rsa modulus 3072  crypto key generate ec keysize <256   384> exportable	Section 4.6.4.1	Clock Management	A series of CLI commands are provided for configuration	Section 4.3
Administrative Activity	Method (Command/GUI Configuration)	Section																																		
Startup/shutdown of the Audit Function	A series of CLI commands is provided for configuration	Section 3.3.3																																		
Terminating session	Exit Logout	Section 3.3.1																																		
Display system information	show version	Section 2 - Step 11																																		
Login Banner	banner login d This is a banner d	Section 4.5																																		
Session Termination	exec-timeout <time>	Section 3.2.5																																		
Lockout configuration	aaa local authentication attempts max-fail [ <i>number of failures</i> ]	Section 3.2.6																																		
Setting Password Length	security passwords min-length <i>length</i>	Section 4.2																																		
Creating Users	username <name> password <password>	Section 3.2.4																																		
Management of Crypto Keys	crypto key generate rsa modulus 3072  crypto key generate ec keysize <256   384> exportable	Section 4.6.4.1																																		
Clock Management	A series of CLI commands are provided for configuration	Section 4.3																																		

Creation of the CSR	A series of CLI commands are provided for configuration	Section 4.6.4.2
Authenticating the Certificate Authority	crypto ca authenticate <i>trustpoint-name</i>	Section 4.6.4.4
Configuring a Revocation Mechanism	revocation-check crl	Section 4.6.4.6
Configuring SSH	A series of CLI commands are provided for configuration	Section 3.3.1
Configuring IKE/IPsec and VPN gateway functionality	A series of CLI commands are provided for configuration	Section 4.6
Configuring MACsec functionality	A series of CLI commands are provided for configuration	Section 3.3.8

Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found.

Administrative Activity	Method (Command/GUI Configuration)	Test Case(s)
Startup/shutdown of the Audit Function	A series of CLI commands are provided for configuration	FAU_GEN.1 T1
Terminating session	Exit Logout	FTA_SSL.4 T1 FTA_SSL.4 T2
Display system information	show version	FPT_TUD_EXT.1 T1
Login Banner	banner login d This is a banner d	FTA_TAB.1 T1
Session Termination	exec-timeout <time>	FTA_SSL_EXT.1 T1 FTA_SSL.3 T1
Lockout configuration	aaa local authentication attempts max-fail [ <i>number of failures</i> ]	FIA_AFL.1 T1 FIA_AFL.1 T2
Setting Password Length	security passwords min-length <i>length</i>	FIA_PMG_EXT.1 T1
Creating Users	username <name> password <password>	FIA_PMG_EXT.1 T1
Management of Crypto Keys	crypto key generate rsa modulus 3072  crypto key generate ec keysize <256   384> exportable	FCS_IPSEC_EXT.1.13 T1 FMT_MTD.1/CryptoKeys T2
Clock Management	A series of CLI commands are provided for configuration	FPT_STM_EXT.1 T1
Creation of the CSR	A series of CLI commands are provided for configuration	FIA_X509_EXT.3 T1
Authenticating the Certificate Authority	crypto ca authenticate <i>trustpoint-name</i>	FIA_X509_EXT.1.1/Rev T1

	Configuring a Revocation Mechanism	revocation-check cri	FCS_IPSEC_EXT.2 T1
	Configuring SSH	A series of CLI commands are provided for configuration	FCS_SSHS_EXT.1.4 T1
	Configuring IKE/IPsec and VPN gateway functionality	A series of CLI commands are provided for configuration	FCS_IPSEC_EXT.1.1 T1
	Configuring MACsec functionality	A series of CLI commands are provided for configuration	FCS_MACSEC_EXT.1 T1 FCS_MKA_EXT.1 T1
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.1.1.7 FAU\_GEN.1 Guidance 3 (VPNGWMod)

Objective	The evaluator shall verify that the operational guidance describes how to configure the TSF to result in applicable network traffic logging. Note that this activity may be addressed in conjunction with the guidance Evaluation Activities for FPF_RUL_EXT.1.
Evaluator Findings	<p>The evaluator examined the section titled <b>Base Firewall Rule Set Configuration</b> in the AGD to verify that it provides information on how to configure the TSF to result in applicable network traffic logging. Upon investigation, the evaluator found that the AGD describe the ability to configure firewall rules on the TOE, using the <b>access-list</b> and <b>ip access-group</b> commands.</p> <p>The evaluator re-examined the section titled <b>Base Firewall Rule Set Configuration</b> in the AGD and found that it contains a description of how to configure logging associated with auditing. Upon investigation, it was found that AGD states</p> <p><b>The logging of matching traffic is done by appending the key word “log-input” per the command reference at the end of the acl statements.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.2 FAU\_STG.1

5.1.2.1 FAU\_STG.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally and how these records are protected against unauthorized modification or deletion. The evaluator shall ensure that the TSS describes the conditions that must be met for authorized deletion of audit records.
Evaluator Findings	<p>The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the amount of audit data that are stored locally, how these records are protected against unauthorized modification or deletion, and the conditions that must be met for authorized deletion of audit records. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE is configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no</b></p>

	<p><b>longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.</b></p> <p><b>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</b></p> <p><b>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 5.1.3 FAU\_STG\_EXT.1

#### 5.1.3.1 FAU\_STG\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	<p>The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE is configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.1.3.2 FAU\_STG\_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	<p>The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space.</b></p>

	<p><b>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.3 FAU\_STG\_EXT.1 TSS 3

Objective	<p>The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.4 FAU\_STG\_EXT.1 TSS 4

Objective	<p>The evaluator shall examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that :</p> <p><b>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space.</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.5 FAU\_STG\_EXT.1 TSS 5

Objective	The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.
Evaluator Findings	The evaluator examined the section titled <b>FAU_STG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in Realtime or periodically. Upon investigation, the evaluator found that the TSS states that:  <b>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.6 FAU\_STG\_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	The evaluator examined the section titled <b>Logging Configuration</b> and <b>Logging Protection</b> in the AGD to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. Upon investigation, the evaluator found that the AGD states that:  <b>If an authorized administrator wants to back up the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:</b>  <ol style="list-style-type: none"> <li>1. <b>With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or</b></li> <li>2. <b>With a syslog server not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.</b></li> </ol> <b>When a Syslog server is configured on the TOE, generated audit events are simultaneously sent to the external server and the local logging buffer.</b> Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.1.3.7 FAU\_STG\_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.
Evaluator Findings	The evaluator examined the section titled <b>Logging Protection</b> in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that:  <b>When a Syslog server is configured on the TOE, generated audit events are simultaneously sent to the external server and the local logging buffer.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.8 FAU\_STG\_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled <b>Security Relevant Events</b> in the AGD and the section titled <b>Security audit (FAU)</b> in the AGD to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the AGD states that:  <b>The TSF shall <u>[overwrite previous audit records according to the following rule: [the newest audit record will overwrite the oldest audit record.]]</u> when the local storage space for audit data is full.</b>  And the AGD states that,  <b>The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

## 5.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as “Test/CAVP” activities.

5.2.1 FCS\_CKM.1

5.2.1.1 FCS\_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	<p>The evaluator examined the section titled <b>FCS_CKM.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE can create an RSA public-private key pair, with a minimum RSA key size of 3072-bit and ECDSA key pairs using NIST curves P-256 and P-384. Both RSA and ECC schemes can be used to generate a Certificate Signing Request (CSR).</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.1.2 FCS\_CKM.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.
Evaluator Findings	<p>The evaluator examined the section titled <b>Generate a Key Pair</b> in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>RSA and ECDSA keys are generated in pairs—one public key and one private key:</b>  <b>(config)# crypto key generate rsa modulus 3072</b>  <b>- or -</b>  <b>(config)# crypto key generate ec keysizes &lt;256   384&gt; exportable</b></p> <p><b>The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.1.3 FCS\_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	<p>CAVP Certs: # A1462</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass



5.2.2 FCS\_CKM.1.1/IKE

5.2.2.1 FCS\_CKM.1.1/IKE TSS 1

Objective	<p>The evaluator shall check to ensure that the TSS describes how the key-pairs are generated. In order to show that the TSF implementation complies with FIPS PUB 186-4, the evaluator shall ensure that the TSS contains the following information:</p> <ul style="list-style-type: none"> <li>• The TSS shall list all sections of Appendix B to which the TOE complies.</li> <li>• For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options, it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;</li> <li>• For each applicable section of Appendix B, any omission of functionality related to "shall" or "should" statements shall be described.</li> </ul> <p>Any TOE-specific extensions, processing that is not included in the Appendices, or alternative Implementations allowed by the Appendices that may impact the security requirements the TOE is to enforce shall be described.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_CKM.1/IKE</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how the key-pairs are generated. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6 and FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3 and RFC 3526.</b></p> <p><b>Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes and Appendix B.4 for ECDSA schemes.</b></p> <p>The TOE does not claim any 'shall not' statements against FIPS 186-4 and therefore does not require the additional listing of items within the TSS.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.2.2 FCS\_CKM.1.1/IKE Guidance 1

Objective	<p>The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>X.509 Certificates</b> in the AGD to verify that it describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. Upon investigation, the evaluator found that the AGD states that</p>

	<p>The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.</p> <p>Creation of these certificates and loading them on the TOE is covered in [9], and a portion of the TOE configuration for use of these certificates follows below.</p> <p>The evaluator examined the section titled <b>Generate a Key Pair</b> in the AGD to verify that it describes the format and location of the output of the key generation process. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>RSA and ECDSA keys are generated in pairs—one public key and one private key:</b></p> <p style="text-align: center;"> <b>(config)# crypto key generate rsa modulus 3072</b>  <b>- or -</b>  <b>(config)# crypto key generate ec keysize &lt;256   384&gt; exportable</b> </p> <p>The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.2.3 FCS\_CKM.1/IKE Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # <b>A1462</b> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS\_CKM.2

5.2.3.1 FCS\_CKM.2 TSS 1 [TD0580]

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled the <b>FCS_CKM.2</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6. FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3 and RFC 3526.</b></p>

	Scheme	SFR	Service
	RSA Key generation	FCS_SSHS_EXT.1	RSA public key authentication for SSH
		FCS_IPSEC_EXT.1	Support for RSA signature-based authentication
		FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	RSA certificate-based authentication
	ECC Key generation Key establishment	FCS_IPSEC_EXT.1	Transmit generated audit data to an external IT entity  Support for protecting VPN traffic
		FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	ECDSA signature-based authentication
	FFC Key generation Key establishment	FCS_SSHS_EXT.1	Key establishment for SSH
FCS_IPSEC_EXT.1		Syslog Server Key establishment for VPN	
Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass.		

5.2.3.2 FCS\_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	<p>The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Ensure that the product is configured to support diffie-hellman-group14-sha1 key exchange using the following command 'ip ssh dh min size 2048':</b></p> <p style="text-align: center;"><b>TOE-common-criteria(config)# ip ssh dh min size 2048</b></p> <p>The section titled <b>IKEv2 Transform Sets</b> in the AGD mentions the other supported schemes and its configuration. It states that:</p> <p><b>TOE-common-criteria (config-isakmp)# group 14</b></p> <p><b>This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP) and 15 (3072-bit MODP) are also allowed and supported.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

5.2.3.3 FCS\_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
-----------	---

Evaluator Findings	CAVP Certs: #A1462 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.4 FCS\_CKM.4

5.2.4.1 FCS\_CKM.4 TSS 1

Objective	The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for <sup>2</sup> ). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.																							
Evaluator Findings	The evaluator examined the section titled <b>Key Zeroization</b> in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that :																							
	<table border="1"> <thead> <tr> <th>Name</th> <th>Description of Key</th> <th>Zeroization</th> </tr> </thead> <tbody> <tr> <td>Diffie-Hellman Shared Secret</td> <td>This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.</td> <td>Automatically after completion of DH exchange.  Overwritten with: 0x00</td> </tr> <tr> <td>Diffie Hellman private exponent</td> <td>This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.</td> <td>Zeroized upon completion of DH exchange.  Overwritten with: 0x00</td> </tr> <tr> <td>Skeyid</td> <td>This is the IKE intermittent value used to create skeyid_d. This key is stored in SDRAM.</td> <td>Automatically after IKE session terminated.  Overwritten with: 0x00</td> </tr> <tr> <td>skeyid_d</td> <td>This is the IKE intermittent value used to derive keying data for IPsec. This key is stored in SDRAM.</td> <td>Automatically after IKE session terminated.  Overwritten with: 0x00</td> </tr> <tr> <td>IKE session encrypt key</td> <td>This is the IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in SDRAM.</td> <td>Automatically after IKE session terminated.  Overwritten with: 0x00</td> </tr> <tr> <td>IKE session authentication key</td> <td>This is the IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in SDRAM.</td> <td>Automatically after IKE session terminated.  Overwritten with: 0x00</td> </tr> </tbody> </table>			Name	Description of Key	Zeroization	Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Automatically after completion of DH exchange.  Overwritten with: 0x00	Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Zeroized upon completion of DH exchange.  Overwritten with: 0x00	Skeyid	This is the IKE intermittent value used to create skeyid_d. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00	skeyid_d	This is the IKE intermittent value used to derive keying data for IPsec. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00	IKE session encrypt key	This is the IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00	IKE session authentication key	This is the IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00
Name	Description of Key	Zeroization																						
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Automatically after completion of DH exchange.  Overwritten with: 0x00																						
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Zeroized upon completion of DH exchange.  Overwritten with: 0x00																						
Skeyid	This is the IKE intermittent value used to create skeyid_d. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00																						
skeyid_d	This is the IKE intermittent value used to derive keying data for IPsec. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00																						
IKE session encrypt key	This is the IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00																						
IKE session authentication key	This is the IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated.  Overwritten with: 0x00																						

	ISAKMP preshared key	This is the configured preshared key for ISAKMP negotiation. This key is stored in NVRAM.	Zeroized using the following command:  <b># no crypto isakmp key</b>  Overwritten with: 0x0d
	IKE ECDSA Private Key	The ECDSA private-public key pair is created by the device itself using the key generation CLI command.  Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate.  In the IKE authentication step, the device's certificate is firstly sent to other device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. . Only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	Zeroized using the following command:  <b># crypto key zeroize ecdsa<sup>1</sup></b>  Overwritten with: 0x0d
	IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate.  In the IKE authentication step, the device's certificate is firstly sent to other device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. . Only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	Zeroized using the following command:  <b># crypto key zeroize rsa</b>  Overwritten with: 0x0d
	IPSec encryption key	This is the key used to encrypt IPSec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated.  Overwritten with: 0x00
	IPSec authentication key	This is the key used to authenticate IPSec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated.  Overwritten with: 0x00

<sup>1</sup> Issuing this command will zeroize/delete all ECDSA keys on the TOE.

	RADIUS secret	Shared secret used as part of the Radius authentication method. This key is stored in NVRAM.	Zeroized using the following command:  <b># no radius-server key</b>  Overwritten with: 0x0d
	SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command:  <b># crypto key zeroize rsa</b>  Overwritten with: 0x00
	SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This is called by the ssh_close function when a session is ended. This key is stored in SDRAM.	Automatically when the SSH session is terminated.  Overwritten with: 0x00
	MACsec Security Association Key (SAK)	The SAK is used to secure the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  The value is zeroized by overwritten by another key or freed upon session is expired.
	MACsec Connectivity Association Key (CAK)	The CAK secures the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  The value is zeroized by overwritten by another key or freed upon session is expired.
	MACsec Key Encryption Key (KEK)	The Key Encrypting Key (KEK) is used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a Secure Connectivity Association (CA). This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  The value is zeroized by overwritten by another key or freed upon session is expired.
	MACsec Integrity Check Key (ICK)	The ICK is used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, This key is stored in internal ASIC register.	Automatically when MACsec session terminated.  The value is zeroized by overwritten by another key or freed upon session is expired.
	<p>The evaluator examined the section titled <b>Key Zeroization</b> in the Security Target to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs).</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>		
Verdict	Pass		

5.2.4.2 FCS\_CKM.4 TSS 2

Objective	The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and
-----------	---

	description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).
Evaluator Findings	The evaluator examined the <b>FCS_CKM.4</b> entry in section titled <b>TOE Summary Specification</b> and the section titled <b>Key Zeroization</b> in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS states that the table provided information on keys stored in non- volatile memory including a description of the interfaces used to destroy keys.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.2.4.3 FCS\_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
Evaluator Findings	The evaluator examined the section titled <b>Key Zeroization</b> in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that no keys are stored in non-plaintext form.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.2.4.4 FCS\_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the section titled <b>Key Zeroization</b> in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states that TOE zeroizes all secrets, keys, and associated values when they are no longer required. Hence no circumstances were found where destruction may be prevented or delayed.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.2.4.5 FCS\_CKM.4 TSS 5

Objective	Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
-----------	--

Evaluator Findings	The evaluator verified that ST does not specify the use of ‘a value that does not contain any CSP’ to overwrite keys.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.6 FCS\_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the AGD and security Target to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS. Upon investigation, the evaluator found that no items that did not meet conformance to the key destruction requirement.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS\_COP.1/DataEncryption

5.2.5.1 FCS\_COP.1/DataEncryption TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled <b>FCS_COP.1/DataEncryption</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that:  <b>The TOE provides symmetric encryption and decryption capabilities using AES in GCM and CBC mode (128, 192 and 256 bits) as described in ISO 18033-3, ISO 19772 and ISO 10116 respectively. Please see CAVP certificate in Table 7 for validation details. AES is implemented in the IPsec and SSH protocols. The TOE provides AES encryption and decryption in support of IPsec and SSHv2 for secure communications.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.5.2 FCS\_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled <b>IKEv1 Transform Sets, IKEv2 Transform Sets, IPsec Transforms and Lifetimes</b> and <b>Remote Administration Protocols</b> in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected



mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states that:

**TOE-common-criteria (config-isakmp)# encryption aes**

This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC\_192 and AES-CBC-256 can be selected with the encryption command, encryption <aes | aes-192 | aes-256>.

**Note:** the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128.

**Note:** Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.

**TOE-common-criteria (config-ikev2-proposal)# encryption aes-cbc-128**

This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-192, AES-CBC-256, AES-GCM-128, and AES-GCM-256 can be selected with the encryption command, encryption <aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-gcm-128 | aes-gcm-256>.

**Note:** the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).

**Note:** Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

Router(config)# crypto ipsec transform-set NAME <esp-aes 128 | esp-aes 192 | esp-aes 256> <esp-sha-hmac | esp-sha256-hmac | esp-sha512-hmac>

or

Router(config)# crypto ipsec transform-set NAME <esp-gcm 128 | esp-gcm 192 | esp-gcm 256>

**Example command:**

TOE-common-criteria(config)# crypto ipsec transform-set EXAMPLE esp-aes 128 esp-sha-hmac

**Note:** The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting in 4.6.1.1 and 4.6.1.2 above. If AES-CBC-128 was selected there for use with IKE encryption, then only AES-CBC-128 or AES-GCM-128 may be selected here.

To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command:

TOE-common-criteria(config)# ip ssh server algorithm encryption aes128-cbc aes256-cbc

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.5.3 FCS\_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: <b>#A1462, #4550, #4544</b> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6 FCS\_COP.1/SigGen

5.2.6.1 FCS\_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled <b>FCS_COP.1/SigGen</b> in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that  <b>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 3072 and greater as specified in ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.</b> <b>In addition, the TOE will provide cryptographic signature services using ECDSA with key size of 256 and 384 bits as specified in FIPS PUB 186-4, "Digital Signature Standard". The TOE provides cryptographic signature services using ECDSA that meets ISO/IEC 14888-3, Section 6.4 with NIST curves P-256 and P-384.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 FCS\_COP.1/SigGen Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled <b>Setting X.509 for use with IKE</b> in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states that:  Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv1 with the commands:  <b>TOE-common-criteria (config)#crypto isakmp policy 1</b> <b>TOE-common-criteria (config-isakmp)# authentication rsa-sig</b> <b>or</b> <b>TOE-common-criteria (config-isakmp)# authentication ecdsa-sig</b>

	<p><b>And for IKEv2 with the commands:</b></p> <p><b>TOE-common-criteria (config)#crypto ikev2 profile sample</b></p> <p><b>TOE-common-criteria(config-ikev2-profile)#authentication [remote   local] rsa-sig</b></p> <p><b>or</b></p> <p><b>TOE-common-criteria(config-ikev2-profile)#authentication [remote   local] ecdsa-sig</b></p> <p><b>If an invalid certificate is loaded, authentication will not succeed.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.6.3 FCS\_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	<p>CAVP RSA SigGen&amp;SigVer (186-4) Certs: <b>#A1462</b></p> <p>CAVP ECDSA&amp;SigVer SigGen (186-4) Certs: <b>#A1462</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.7 FCS\_COP.1/Hash

5.2.7.1 FCS\_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled <b>FCS_COP.1/Hash</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512 as specified in ISO/IEC 10118-3:2004</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.7.2 FCS\_COP.1/Hash Guidance 1

Objective	The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets</b> and <b>IKEv2 Transform Sets</b> in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The following settings must be set in configuring the IPsec with IKEv1 functionality for the TOE:</b></p>

	<p>TOE-common-criteria # conf t</p> <p>TOE-common-criteria (config)#crypto isakmp policy 1</p> <p>TOE-common-criteria (config-isakmp)# hash sha</p> <p>Thus, the following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:</p> <p>TOE-common-criteria # conf t</p> <p>TOE-common-criteria (config)#crypto ikev2 proposal sample</p> <p>TOE-common-criteria (config-ikev2-proposal)# integrity sha1</p> <p>This configures IPsec IKEv2 to use SHA-1 cryptographic hashing. SHA 256 and SHA-512 can be configured with the integrity command, integrity &lt;sha1   sha256   sha512&gt;.</p> <p>This configures IPsec IKEv1 to use SHA-1 cryptographic hashing. SHA-256 and SHA-512 can be configured with the hash command, hash &lt;sha   sha256   sha512&gt;.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.7.3 FCS\_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: #A1462 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8 FCS\_COP.1/KeyedHash

5.2.8.1 FCS\_COP.1/KeyedHash TSS 1

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	<p>The evaluator examined the section titled <b>FCS_COP.1/KeyedHash</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 and HMAC-SHA-256 operates on 512-bit blocks and HMAC-SHA-512 operate on 1024-bit blocks of data, with key sizes and message digest sizes of 160-bits, 256 bits and 512 bits respectively) as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.8.2 FCS\_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	<p>The evaluator examined the section titled <b>IPsec Transforms and Lifetimes and Remote Administration Protocols</b> in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.</b></p> <p><b>Router(config)# crypto ipsec transform-set NAME &lt;esp-aes 128   esp-aes 192   esp-aes 256&gt; &lt;esp-sha-hmac   esp-sha256-hmac   esp-sha512-hmac&gt;</b></p> <p><b>or</b></p> <p><b>Router(config)# crypto ipsec transform-set NAME &lt;esp-gcm 128   esp-gcm 192   esp-gcm 256&gt;</b></p> <p><b>The TOE also needs to be configured to only support HMAC-SHA2-256 and HMAC-SHA2-512 MAC algorithms using the following:</b></p> <p><b>TOE-common-criteria(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.8.3 FCS\_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	<p>CAVP HMAC Certs: <b>#A1462</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.9 FCS\_COP.1(1)/KeyedHashCMAC

5.2.9.1 FCS\_COP.1(1)/KeyedHashCMAC TSS 1 [TD0466]

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined the <b>FCS_COP.1/KeyedHashCMAC</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that:

	<p>The TOE implements AES-CMAC keyed hash function for message authentication as described in NIST SP 800-38B.</p> <p>The key length, hash function used, block size, and output MAC length used are as follows:</p> <p style="padding-left: 40px;"><b>AES-128 (hash function and key length)</b>  Block Sizes: Full (block size)  Message Length: 0-256 bits (output MAC length)</p> <p style="padding-left: 40px;"><b>AES-256 (hash function and key length)</b>  Block Sizes: Full (block size)  Message Length: 0-256 bits (output MAC length)</p> <p>The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 and 256 bits) as described in AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772.  <b>AES is implemented in MACsec protocol.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.9.2 FCS\_COP.1(1)/KeyedHashCMAC Test/CAVP 1 [TD0466]

Objective	The evaluator shall verify the implementation of Keyed Hash CMAC supported by the TOE.
Evaluator Findings	CAVP AES Certs: #A1462, #4550, #4544 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.10 FCS\_COP.1(2) Cryptographic Operation (MACsec AES Data Encryption/Decryption)

5.2.10.1 FCS\_COP.1(2) TSS 1 [TD0466]

Objective	The evaluator shall verify that the TSS describes the supported AES modes that are required for this EP in addition to the ones already required by the NDcPP.
Evaluator Findings	<p>The evaluator examined the <b>FCS_COP.1(2)</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS to ensure it identifies the mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 and 256 bits) as described in AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772.</b>  <b>AES is implemented in MACsec protocol.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.10.2 FCS\_COP.1(2) Test/CAVP 1 [TD0466]

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: #A1462, #4544, #4550 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.11 FCS\_RBG\_EXT.1

5.2.11.1 FCS\_RBG\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the section titled <b>FCS_RBG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS states that  <b>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source.</b>  <b>The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.11.2 FCS\_RBG\_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the AGD and verified that no configuration is required for implementation of the RNG functionality. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.11.3 FCS\_RBG\_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: #A1462 Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

### 5.3 TSS and Guidance Activities (IPsec)

#### 5.3.1 FCS\_IPSEC\_EXT.1

##### 5.3.1.1 FCS\_IPSEC\_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes what takes place when a packet is processed by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network as specified in RFC 4301.</b></p> <p><b>When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. For example:</b></p> <p style="text-align: center;"><b>Router# crypto map MAP_NAME 10 ipsec-isakmp</b></p> <p><b>The match address 101 command means to use access list 101 in order to determine which traffic is relevant. For example:</b></p> <p style="text-align: center;"><b>Router# (config-crypto-map)#match address 101</b></p> <p><b>The traffic matching the permit acs would then flow through the IPsec tunnel and be classified as "PROTECTED".</b></p> <p><b>Traffic that does not match a permit acl and is also blocked by other non-crypto acs on the interface would be DISCARDED.</b></p> <p><b>Traffic that does not match a permit acl in the crypto map, but that is not disallowed by other acs on the interface is allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass



Objective	<p>As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>A crypto map (the Security Policy Definition (SPD)) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. Separate access lists define blocking and permitting at the interface). For example:</b></p> <pre>Router# access-list 101 permit ip 192.168.3.0 0.0.0.255 10.3.2.0 0.0.0.255</pre> <p><b>When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. For example:</b></p> <pre>Router# crypto map MAP_NAME 10 ipsec-isakmp</pre> <p><b>The match address 101 command means to use access list 101 in order to determine which traffic is relevant. For example:</b></p> <pre>Router# (config-crypto-map)#match address 101</pre> <p><b>The traffic matching the permit acls would then flow through the IPsec tunnel and be classified as "PROTECTED".</b></p> <p><b>Traffic that does not match a permit acl and is also blocked by other non-crypto acls on the interface would be DISCARDED.</b></p> <p><b>Traffic that does not match a permit acl in the crypto map, but that is not disallowed by other acls on the interface is allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit crypto map was not configured that matches the ping traffic.</b></p> <p><b>If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.3.1.3 FCS\_IPSEC\_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.
Evaluator Findings	<p>The evaluator examined the section titled <b>IPSec Overview</b> in the AGD to verify that it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry.</b></p> <p><b>When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.</b></p> <p><b>Access lists associated with IPsec crypto map entries also represent the traffic that the router needs protected by IPsec. Inbound traffic is processed against crypto map entries--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.</b></p> <p><b>Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.4 FCS\_IPSEC\_EXT.1.3 TSS 1

Objective	The evaluator checks the TSS to ensure it states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3).
Evaluator Findings	The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS states that the VPN can be

	<p>established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3). Upon investigation, the evaluator found that the TSS states that:</p> <p><b>In addition to tunnel mode, which is the default IPsec mode, the TOE also supports transport mode, allowing for only the payload of the packet to be encrypted. If tunnel mode is explicitly specified, the router will request tunnel mode and will accept only tunnel mode.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.5 FCS\_IPSEC\_EXT.1.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions on how to configure the connection in each mode selected.
Evaluator Findings	<p>The evaluator examined the entry in section titled titled <b>IPsec Transforms and Lifetimes</b> in the AGD to verify that it contains instructions on how to configure the connection in each mode selected. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>TOE-common-criteria (config-isakmp)# crypto isakmp aggressive-mode disable</b></p> <p><b>Main mode is the default mode and the crypto isakmp aggressive-mode disable ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.</b></p> <p><b>TOE-common-criteria(config-isakmp)#exit</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.6 FCS\_IPSEC\_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that the selected algorithms are implemented. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1/KeyedHash Cryptographic Operations (for keyed-hash message authentication) and if the SHA-based HMAC function truncated output is utilized it must also be described.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS states that the selected algorithms are implemented. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. The IPsec protocol ESP, as defined by RFC 4303, is implemented using the cryptographic algorithms AES-CBC-128 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106) and AES-CBC-192 (RFC 3602), AES-GCM-192 (RFC 4106) together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-512.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.3.1.7 FCS\_IPSEC\_EXT.1.4 Guidance 1

Objective	The evaluator checks the guidance documentation to ensure it provides instructions on how to configure the TOE to use the algorithms selected.
Evaluator Findings	<p>The evaluator examined the section titled <b>IPsec Transforms and Lifetimes</b> in the AGD to verify that it provides instructions on how to configure the TOE to use the algorithms selected. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.</b></p> <p><b>Router(config)# crypto ipsec transform-set NAME &lt;esp-aes 128   esp-aes 192   esp-aes 256&gt; &lt;esp-sha-hmac   esp-sha256-hmac   esp-sha512-hmac&gt;</b></p> <p><b>Or</b></p> <p><b>Router(config)# crypto ipsec transform-set NAME &lt;esp-gcm 128   esp-gcm 192   esp-gcm 256&gt;</b></p> <p><b>Example command:</b></p> <p><b>TOE-common-criteria(config)# crypto ipsec transform-set EXAMPLE esp-aes 128 esp-sha-hmac</b></p> <p><b>Note: The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting in 4.6.1.1 and 4.6.1.2 above. If AES-CBC-128 was selected there for use with IKE encryption, then only AES-CBC-128 or AES-GCM-128 may be selected here.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.8 FCS\_IPSEC\_EXT.1.5 TSS 1

Objective	The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies whether IKEv1 and/or IKEv2 are implemented. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE supports both IKEv1 and IKEv2 session establishment.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.9 FCS\_IPSEC\_EXT.1.5 TSS 2

Objective	For IKEv1 implementations, the evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the ‘crypto ISAKMP aggressive-mode disable’ command</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.10 FCS\_IPSEC\_EXT.1.5. Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected).
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets, IKEv2 Transform Sets and NAT Traversal</b> in the AGD to verify that it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected). Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The following settings must be set in configuring the IPsec with IKEv1 functionality for the TOE:</b></p> <p><b>TOE-common-criteria # conf t</b></p> <p><b>TOE-common-criteria (config)#crypto isakmp policy 1</b></p> <p><b>TOE-common-criteria (config-isakmp)# hash sha</b></p> <p><b>This configures IPsec IKEv1 to use SHA-1 cryptographic hashing. SHA-256 and SHA-512 can be configured with the hash command, hash &lt;sha   sha256   sha512&gt;.</b></p> <p><b>TOE-common-criteria (config-isakmp)# encryption aes</b></p> <p><b>This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC_192 and AES-CBC-256 can be selected with the encryption command, encryption &lt;aes   aes-192   aes-256&gt;.</b></p> <p><b>Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128.</b></p> <p><b>Note: Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.</b></p> <p>In addition to this for IKEv1, commands for configuring the authentication method, pre-shared keys, DH group, lifetime and aggressive mode are stated in the AGD.</p>

	<p>The following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:</p> <pre>TOE-common-criteria # conf t TOE-common-criteria (config)#crypto ikev2 proposal sample TOE-common-criteria (config-ikev2-proposal)# integrity sha1</pre> <p>This configures IPsec IKEv2 to use SHA-1 cryptographic hashing. SHA 256 and SHA-512 can be configured with the integrity command, integrity &lt;sha1   sha256   sha512&gt;.</p> <pre>TOE-common-criteria (config-ikev2-proposal)# encryption aes-cbc-128</pre> <p>This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-192, AES-CBC-256, AES-GCM-128, and AES-GCM-256 can be selected with the encryption command, encryption &lt;aes-cbc-128   aes-cbc-192   aes-cbc-256   aes-gcm-128   aes-gcm-256&gt;.</p> <p><b>Note:</b> the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).</p> <p><b>Note:</b> Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.</p> <p>In addition to this for IKEv2, commands for configuring the authentication method, pre-shared keys, DH group, lifetime and keyring are stated in the AGD.</p> <p><b>For successful NAT traversal over an IOS-XE NAT device for an IPsec connection between two IOS-XE peers, the following configuration needs to be used</b></p> <p><b><u>On an IOS NAT device (router between the IPsec endpoints):</u></b></p> <pre>config terminal ip nat service list &lt;ACL-number&gt; ESP spi-match access-list &lt;ACL-number&gt; permit &lt;protocol&gt; &lt;local-range&gt; &lt;remote-range&gt; end</pre> <p><b><u>On each IOS peer (IPsec router endpoints):</u></b></p> <pre>config terminal crypto ipsec nat-transparency spi-matching end</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.11 FCS\_IPSEC\_EXT.1.5. Guidance 2

Objective	If the IKEv1 Phase 1 mode requires configuration of the TOE prior to its operation, the evaluator shall check the guidance documentation to ensure that instructions for this configuration are contained within that guidance.
Evaluator Findings	The evaluator examined the section titled <b>IKEv1 Transform Sets</b> in the AGD to verify that it contains any necessary instructions for IKEv1 Phase 1 mode configuration. Upon investigation, the evaluator found that the AGD states that:

	<p><b>TOE-common-criteria (config-isakmp)# crypto isakmp aggressive-mode disable</b></p> <p><b>Main mode is the default mode and the crypto isakmp aggressive-mode disable ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.</b></p> <p><b>TOE-common-criteria(config-isakmp)#exit</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.12 FCS\_IPSEC\_EXT.1.6 TSS 1

Objective	The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE provides AES-CBC-128, AES-CBC-192 and AES-CBC-256 for encrypting the IKEv1 payloads, and AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192 and AES-GCM-256 for IKEv2 payloads. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.13 FCS\_IPSEC\_EXT.1.6 Guidance 1

Objective	The evaluator ensures that the guidance documentation describes the configuration of all selected algorithms in the requirement.
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets ,IKEv2 Transform Sets</b> in the AGD to verify that it describes the configuration of all selected algorithms in the requirement. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>TOE-common-criteria (config-isakmp)# encryption aes</b></p> <p><b>This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC_192 and AES-CBC-256 can be selected with the encryption command, encryption &lt;aes   aes-192   aes-256&gt;.</b></p> <p><b>Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128.</b></p> <p><b>TOE-common-criteria (config-isakmp)# hash sha</b></p> <p><b>This configures IPsec IKEv1 to use SHA-1 cryptographic hashing. SHA-256 and SHA-512 can be configured with the hash command, hash &lt;sha   sha256   sha512&gt;.</b></p>

	<p><b>Note: Both confidentiality and integrity are configured with the hash and encryption commands</b></p> <p><b>TOE-common-criteria (config-ikev2-proposal)# encryption aes-cbc-128</b></p> <p>This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-192, AES-CBC-256, AES-GCM-128, and AES-GCM-256 can be selected with the encryption command, encryption &lt;aes-cbc-128   aes-cbc-192   aes-cbc-256   aes-gcm-128   aes-gcm-256&gt;.</p> <p><b>Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).</b></p> <p><b>Note: Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.14 FCS\_IPSEC\_EXT.1.7 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime and that information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.15 FCS\_IPSEC\_EXT.1.7 Guidance 1 [TD0633]

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is performed no later than 24h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for
-----------	---



	the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets, IKEv2 Transform Sets</b> in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>TOE-common-criteria (config-isakmp)# lifetime 86400</b>  <b>The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values</b></p> <p><b>TOE-common-criteria (config-ikev2-proposal)# lifetime 86400</b>  <b>The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.16 FCS\_IPSEC\_EXT.1.8 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime and that the information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets.</b></p> <p><b>The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.17 FCS\_IPSEC\_EXT.1.8 Guidance 1 [TD0633]

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the Guidance documentation allows the Administrator to
-----------	--

	configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	<p>The evaluator examined the section titled <b>IPsec Transforms and Lifetimes</b> in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that</p> <p><b>TOE-common-criteria (config)#crypto ipsec security-association lifetime seconds 28800</b></p> <p><b>The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour. There is no configuration required for these since the defaults are acceptable. However, to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above.</b></p> <p><b>TOE-common-criteria (config)#crypto ipsec security-association lifetime kilobytes 100000</b></p> <p><b>This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.18 FCS\_IPSEC\_EXT.1.9 TSS 1

Objective	The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x". The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" meets the stipulations in the requirement.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the process for generating "x" for each DH group supported. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), and 15 (3072-bit MODP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, Table 2 in NIST SP 800-57 "Recommendation for Key Management –Part 1: General" and the following corresponding key sizes (in bits) are used: 224 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), 384 (for DH Group 20) and 256 (for DH Group 15) bits.</b></p> <p><b>The secret value 'x' used in the IKE Diffie-Hellman key exchange ("x" in <math>g^x \text{ mod } p</math>) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG).</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.19 FCS\_IPSEC\_EXT.1.10 TSS 1

Objective	<p>If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.</p> <p>If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the process for generating each nonce for each DH group or PRF hash supported and indicates that the random number generated that meets the requirements in this PP is used and indicates that the length of the nonces meet the stipulations in the requirement. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE supports Diffie-Hellman Group 14, 19, 24, 20 and 15. Group 14 (2048-bit keys) can be set by using the “group 14” command in the config mode. The nonces used in IKE exchanges are generated in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2<sup>128</sup>.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.20 FCS\_IPSEC\_EXT.1.11 TSS 1

Objective	<p>The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists the DH groups specified in the requirement as being supported. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), and 15 (3072-bit MODP) in support of IKE Key Establishment.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.21 FCS\_IPSEC\_EXT.1.11 Guidance 1

Objective	<p>The evaluator ensures that the guidance documentation describes the configuration of all algorithms selected in the requirement.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets</b> and <b>IKEv2 Transform Sets</b> in the AGD to verify that it describes the configuration of all algorithms selected in the requirement. Upon investigation, the evaluator found that the AGD states that</p>

	<p><b>TOE-common-criteria (config-isakmp)# group 14</b></p> <p>This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP) and 15 (3072 bit MODP) are also allowed and supported</p> <p><b>TOE-common-criteria (config-ikev2-proposal)# group 14</b></p> <p>This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), and 15 (3072 bit MODP) are also allowed and supported.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.22 FCS\_IPSEC\_EXT.1.12 TSS 1

Objective	<p>The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the potential strengths of the algorithms that are allowed for the IKE and ESP exchanges and the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 1 and IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection.</b></p> <p><b>IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including:</b></p> <ul style="list-style-type: none"> <li>• <b>The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based, or pre-shared key based),</b></li> <li>• <b>The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and</b></li> <li>• <b>The agreement of secure bulk data encryption AES keys for use with ESP.</b></li> </ul> <p><b>After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation.</b></p> <p><b>The TOE provides AES-CBC-128, AES-CBC-192 and AES-CBC-256 for encrypting the IKEv1 payloads, and AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192 and AES-GCM-256 for IKEv2 payloads. The administrator is instructed in the AGD to ensure that</b></p>

	<p><b>the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.23 FCS\_IPSEC\_EXT.1.13 TSS 1

Objective	The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1/SigGen Cryptographic Operations (for cryptographic signature).
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication and that the algorithms are consistent with those specified in FCS_COP.1/SigGen Cryptographic Operations. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The IKE protocols implement Peer Authentication using RSA and ECDSA along with X.509v3 certificates, or pre-shared keys.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.24 FCS\_IPSEC\_EXT.1.13 TSS 2

Objective	If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. Upon investigation, the evaluator found that the TSS states that</p> <p><b>Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.25 FCS\_IPSEC\_EXT.1.13 Guidance 1

Objective	The evaluator ensures the guidance documentation describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys.
Evaluator Findings	The evaluator examined the section titled <b>X.509 Certificates</b> and <b>Setting X.509 for use with IKE</b> in the AGD to verify that it describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys. Upon investigation, the evaluator found that the AGD states that

	<p>The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.</p> <p>Creation of these certificates and loading them on the TOE is covered in [9], and a portion of the TOE configuration for use of these certificates follows below.</p> <p>Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv1 with the commands:</p> <p>TOE-common-criteria (config)#crypto isakmp policy 1</p> <p>TOE-common-criteria (config-isakmp)# authentication rsa-sig</p> <p>or</p> <p>TOE-common-criteria (config-isakmp)# authentication ecdsa-sig</p> <p>And for IKEv2 with the commands:</p> <p>TOE-common-criteria (config)#crypto ikev2 profile sample</p> <p>TOE-common-criteria(config-ikev2-profile)#authentication [remote   local] rsa-sig</p> <p>or</p> <p>TOE-common-criteria(config-ikev2-profile)#authentication [remote   local] ecdsa-sig</p> <p>If an invalid certificate is loaded, authentication will not succeed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.26 FCS\_IPSEC\_EXT.1.13 Guidance 2

Objective	<p>The evaluator shall check that the guidance documentation describes how preshared keys are to be generated and established. The description in the guidance documentation shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets</b> and <b>IKEv2 Transform Sets</b> in the AGD to verify that it describes how pre-shared keys are to be generated and established. Upon investigation, the evaluator found that the AGD states that</p> <p><b><u>IKEV1</u></b></p> <p><b>TOE-common-criteria (config-isakmp)# authentication pre-share</b></p> <p><b>This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.</b></p> <p><b>TOE-common-criteria(config-isakmp)# Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4</b></p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "\$", "%", "^", "&amp;", "*", "(", and ").").</b></p>

	<p>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.</p> <p><b><u>IKEV2</u></b></p> <p><b>TOE-common-criteria (config-ikev2-proposal)# authentication local pre-share</b></p> <p>This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.</p> <p><b>TOE-common-criteria (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC</b></p> <p>This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.</p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “”).</b></p> <p>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, but longer keys increase processing time.</p> <p>HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: ‘pre-shared-key hex [hex key]’.</p> <p>For example: pre-shared-key hex 0x6A6B6C.</p> <p>This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.27 FCS\_IPSEC\_EXT.1.13 Guidance 3

Objective	<p>The evaluator will ensure that the guidance documentation describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>Authenticating the Certificate Authority</b> in the AGD to verify that it describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint. The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site.</b></p> <p><b>Authenticate the CA: crypto ca authenticates trustpoint-name</b></p> <p><b>Device (config)#crypto ca authenticate ciscotest</b></p> <p><b>Certificate has the following attributes:</b></p> <p><b>Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217 Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280</b></p>



	<p><b>% Do you accept this certificate? [yes/no]: yes</b></p> <p><b>Trustpoint CA certificate accepted.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.28 FCS\_IPSEC\_EXT.1.14 TSS 1

Objective	<p>The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). If the TOE simultaneously supports the same identifier type in the CN and SAN, the TSS shall describe how the TOE prioritizes the comparisons (e.g. the result of comparison if CN matches but SAN does not). If the location (e.g. CN or SAN) of non-DN identifier types must explicitly be configured as part of the reference identifier, the TSS shall state this. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate, including what field(s) are compared and which fields take precedence in the comparison.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_IPSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. Upon investigation, the evaluator found that the TSS states that</p> <p><b>When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used as verification where the attributes in the certificate are compared with the expected CN: FQDN, CN: user FQDN and CN: IP Address.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.29 FCS\_IPSEC\_EXT.1.14 Guidance 1

Objective	<p>The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE does not guarantee unique identifiers, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>Configure Reference Identifier</b> in the AGD to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). Upon investigation, the evaluator found that the AGD states that:</p> <p><b>When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the</b></p>



	<p>attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used as verification where the attributes in the certificate are compared with the expected CN: FQDN, CN: user FQDN and CN: IP Address.</p> <p>This section describes configuration of the peer reference identifier which is achieved through configuring the DN attributes with a certificate map. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and greater than or equal. ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication.</p> <p><b>Note: SAN is not supported for reference identifiers</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 5.4 TSS and Guidance Activities (MACsec)

### 5.4.1 FCS\_MACSEC\_EXT.1

#### 5.4.1.1 FCS\_MACSEC\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE implements MACsec in compliance with IEEE Standard 802.1AE-2006. The MACsec connections maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.1.2 FCS\_MACSEC\_EXT.1 TSS 2

Objective	The evaluator shall also determine that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The SCI is composed of a globally unique 48-bit MAC Address and the Secure System Address (port). The SCI is part of the SecTAG if the SC bit is set and will be at the end of the</b></p>

	<p><b>tag. Any MPDUs during a given session that contain an SCI other than the one used to establish that session are rejected. Only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5) and MAC control frames (EtherType 88-08) are permitted, and others are rejected.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.1.3 FCS\_MACSEC\_EXT.1 TSS 3 [TD0553]

Objective	The evaluator shall check the TSS for an assertion that only EAPOL, MACsec Ethernet frames, and MAC control frames are accepted by the MACsec interface.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS asserts that only EAPOL and MACsec Ethernet frames are accepted by the MACsec interface. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>MACsec connections maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices. Only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5) and MAC control frames (EtherType 88-08) are permitted, and others are rejected.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.2 FCS\_MACSEC\_EXT.2

##### 5.4.2.1 FCS\_MACSEC\_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.2</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 through the CLI command of “mka-policy confidentiality-offset command”.</b></p> <p><b>An offset value of 0 does not offset the encryption and offset values of 30 and 50 offset the encryption by 30 and 50 characters respectively.</b></p> <p><b>An Integrity Check Value (ICV) that is 16 bytes in length is derived with the Secure Association Key (SAK) and is used to provide assurance of the integrity of MPDUs.</b></p>

	<p><b>The TOE derives the ICV from a CAK using KDF, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.2.2 FCS\_MACSEC\_EXT.2 Guidance 1

Objective	<p>If any integrity verifications are configurable such as the confidentiality offset(s) used or the mechanism used to derive an ICK, the evaluator shall verify that instructions for performing these functions are documented.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>MACsec and MKA Configuration</b> in the AGD to verify that, if any integrity verifications are configurable such as the confidentiality offset(s) used or the mechanism used to derive an ICK, it documents instructions for performing these functions. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in [16]:</b></p> <p><a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html</a></p> <p><b>Under section “How to Configure WAN MACsec and MKA Support Enhancements”, there is a sub-section for “Configuring MKA”. This section provides the required instructions for performing functions such as configuring confidentiality offset.</b></p> <ul style="list-style-type: none"> <li>• <b>Configuration of the confidentiality offset, using the confidentiality-offset &lt;&gt; command</b></li> <li>• <b>Configuration of the Integrity Check Value (ICV), using the include-icv-indicator command</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.3 FCS\_MACSEC\_EXT.3

##### 5.4.3.1 FCS\_MACSEC\_EXT.3 TSS 1

Objective	<p>The evaluator shall examine the TSS to verify that it describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK’s key space are provided.</p>
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.3</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK’s key space are provided. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Each SAK is generated using the KDF specified in IEEE 802.1X-2010 section 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from</b></p>

	<p>an RNG each time an SAK is generated. The TOE's random bit generator is used for creating these unique nonces.</p> <p>Each of the keys used by MKA is derived from the CAK. The key string is the CAK that is used for ICV validation by the MKA protocol. The CAK is not used directly but derives two further keys from the CAK using the AES cipher in CMAC mode. The derived keys are tied to the identity of the CAK, and thus restricted to use with that particular CAK. These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by the Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA. The size of the key is based on the configured AES key sized used. If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.4 FCS\_MACSEC\_EXT.4

##### 5.4.4.1 FCS\_MACSEC\_EXT.4 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the SAK is wrapped prior to being distributed using the AES implementation specified in this EP.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MACSEC_EXT.4</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how the SAK is wrapped prior to being distributed using the AES implementation specified. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The SAKs are distributed between these peers using AES Key Wrap. Prior to distribution of the SAKs between these peers, the TOE uses AES Key Wrap in accordance with AES as specified in ISO 18033-3, AES in CMAC mode as specified in NIST SP 800-38B, and GCM as specified in ISO 19772.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### 5.4.4.2 FCS\_MACSEC\_EXT.4 Guidance 1

Objective	The evaluator shall verify that the guidance provides instructions on how to configure peer authentications. The evaluator shall also verify that the method of specifying a lifetime for CAKs is described.
Evaluator Findings	<p>The evaluator examined section titled <b>MACsec and MKA Configuration</b> in the AGD to verify that it provides instructions on how to configure peer authentications and describes the method of specifying a lifetime for CAKs. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in [16]:</b></p> <p><a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/x-17/macsec-xe-17-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/x-17/macsec-xe-17-book.html</a></p>

	<p><b>Under “Configuring MKA Preshared Key (PSK)”, proper guidance has provided to configure peer authentication, and lifetime for CAK respectively.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.5 FCS\_MKA\_EXT.1

##### 5.4.5.1 FCS\_MKA\_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MKA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key.</b></p> <p><b>For the Data Integrity Check, MACsec uses MKA to generate an Integrity Check Value (ICV) for the frame arriving on the port. If the generated ICV is the same as the ICV in the frame, then the frame is accepted; otherwise, it is dropped. The key string is the Connectivity Association Key (CAK) that is used for ICV validation by the MKA protocol.</b></p> <p><b>The Key Server generates a new group CAK when CLI management commands are executed. The Key Server distributes a SAK by pairwise CAKs.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

##### 5.4.5.2 FCS\_MKA\_EXT.1.8 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE’s compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MKA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the TOE’s compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014. The data delay protection is enabled for MKA as a protection guard against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their PDUs. The Delay protection does not operate if and</b></p>

	<p><b>when MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds is enforced by the TOE.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.5.3 FCS\_MKA\_EXT.1.8 TSS 2

Objective	The evaluator shall also verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group's membership changes.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MKA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group's membership changes. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.8 in Section 5.3.2.15. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.8 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.</b></p> <p><b>On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key.</b></p> <p><b>The Key Server generates a new group CAK when CLI management commands are executed. The Key Server distributes a SAK by pairwise CAKs.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.4.5.4 FCS\_MKA\_EXT.1.8 TSS 3

Objective	The evaluator shall also verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4.
Evaluator Findings	<p>The evaluator examined the <b>FCS_MKA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.8 in Section 5.3.2.15. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.8 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.4.5.5 FCS\_MKA\_EXT.1.8 Guidance 1

Objective	The evaluator shall verify that the guidance documentation provides instructions on how to configure the TOE to act as the Key Server in an environment with multiple MACsec-capable devices.
Evaluator Findings	<p>The evaluator examined the section titled <b>MACsec and MKA Configuration</b> in the AGD to verify that it provides instructions on how to configure the TOE to act as the Key Server in an environment with multiple MACsec-capable devices. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in [16]:</b></p> <p><a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html</a></p> <p><b>Under section “How to Configure WAN MACsec and MKA Support Enhancements”, there is a sub-section for “Configuring MKA”. This section provides the required instructions for performing functions such as configuring confidentiality offset.</b></p> <ul style="list-style-type: none"> <li>• <b>Configuration of the key server, using the key-server priority &lt;key-server-priority&gt; command</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 5.5 TSS and Guidance Activities (SSH)

### 5.5.1 FCS\_SSHS\_EXT.1

#### 5.5.1.1 FCS\_SSHS\_EXT.1.2 TSS 1 [TD0631]

Objective	<p>The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).</p> <p>The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client’s presented public key matches one that is stored within the SSH server’s authorized_keys file.</p> <p>If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.</p>
Evaluator Findings	The evaluator examined the <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that:



	<p>The TOE implementation of SSHv2 complies with RFCs 4251, 4252, 4253, 4254, 6668, 8308 section 3.1, 8332 and SSHv2 supports the following:</p> <ul style="list-style-type: none"> <li>• <b>Public key algorithms for authentication: RSA Signature Verification.</b></li> <li>• <b>When an SSH client presents a public key, the TOE establishes a user identity by verifying that the SSH client’s presented public key matches one that is stored within an authorized keys file.</b></li> <li>• <b>Local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server.</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.2 FCS\_SSHS\_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	<p>The evaluator examined <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Packets greater than 65,535 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation, and dropped internal to the SSH process</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.3 FCS\_SSHS\_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	<p>The evaluator examined the <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Encryption algorithms, AES-CBC-128, AES-CBC-256 to ensure confidentiality of the session.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.4 FCS\_SSHS\_EXT.1.4 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
-----------	---



Evaluator Findings	<p>The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command:</b></p> <p><b>TOE-common-criteria(config)# ip ssh server algorithm encryption aes128-cbc aes256-cbc</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.5 FCS\_SSHS\_EXT.1.5 TSS 1 [TD0631]

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server’s host public key algorithms supported are specified and that they are identical to those listed for this component.
Evaluator Findings	<p>The evaluator examined <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states that:</p> <ul style="list-style-type: none"> <li>• <b>Public key algorithms for authentication: RSA Signature Verification.</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.6 FCS\_SSHS\_EXT.1.5 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	<p>The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Generate RSA – choose a longer modulus length for the evaluated configuration (i.e., 3072):</b></p> <p><b>TOE-common-criteria(config)# crypto key generate rsa</b></p> <p><b>How many bits in the modulus [512]: 3072</b></p> <p><b>RSA keys are generated in pairs—one public key and one private key. This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</b></p> <p><b>Note: Only one set of keys can be configured using the crypto key generate command at a time. Repeating the command overwrites the old keys.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.5.1.7 FCS\_SSHS\_EXT.1.6 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: <ul style="list-style-type: none"> <li>• <b>The TOE’s implementation of SSHv2 supports hashing algorithms hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session.</b></li> </ul> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.8 FCS\_SSHS\_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).
Evaluator Findings	The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that: <p><b>The TOE also needs to be configured to only support HMAC-SHA2-256 and HMAC-SHA2-512 MAC algorithms using the following:</b></p> <p><b>TOE-common-criteria(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512</b></p> <p><b>The evaluator also verified that “none” MAC algorithm is not mentioned in the supported list.</b></p> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.9 FCS\_SSHS\_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: <p><b>The TOE’s implementation of SSHv2 can be configured to only allow Diffie-Hellman Group 14 (2048-bit keys) Key Establishment, as required by the PP.</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.10 FCS\_SSHS\_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that:  <b>Ensure that the product is configured to support diffie-hellman-group14-sha1 key exchange using the following command 'ip ssh dh min size 2048':</b> <b>TOE-common-criteria(config)# ip ssh dh min size 2048</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.11 FCS\_SSHS\_EXT.1.8 TSS 1

Objective	The evaluator shall check that the TSS specifies the following:  a) Both thresholds are checked by the TOE. b) Rekeying is performed upon reaching the threshold that is hit first.
Evaluator Findings	The evaluator examined the <b>FCS_SSHS_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS specifies that both thresholds are checked, and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that:  <b>The TOE can also be configured to ensure that SSH re-key of no longer than one hour and no more than one gigabyte of transmitted data for the session key.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.12 FCS\_SSHS\_EXT.1.8 Guidance 1

Objective	If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.
Evaluator Findings	The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that:

	<p><b>Configure the SSH rekey time-based rekey (in minutes) and volume-based rekey values (in kilobytes) (values can be configured to be lower than the default values if a shorter interval is desired):</b></p> <ul style="list-style-type: none"> <li>a. ip ssh rekey time 60</li> <li>b. ip ssh rekey volume 1000000</li> </ul> <p><b>Note: When configuring an SSH rekey time or volume interval, the TOE will begin re-key based upon the first threshold reached</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 5.6 TSS and Guidance Activities (Identification and Authentication)

### 5.6.1 FIA\_AFL.1

#### 5.6.1.1 FIA\_AFL.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>FIA_AFL.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentications attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command. While the TOE supports a range from 1-25, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3. All successive unsuccessful authentication attempts are logged on the router.</b></p> <p><b>When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative CLI.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.1.2 FIA\_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).
Evaluator Findings	The evaluator examined the section titled <b>FIA_AFL.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that  <b>Administrator lockouts are not applicable to the local console.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 FIA\_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.						
Evaluator Findings	The evaluator examined the section titled <b>User Lockout</b> in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). Upon investigation, the evaluator found that the AGD states that:  <b>User accounts must be configured to lockout after a specified number of authentication failures TOE-common-criteria(config)# aaa local authentication attempts max-fail [number of failures]</b>  <b>where number of failures is the number of consecutive failures that will trigger locking of the account. Configuration of these settings is limited to the privileged administrator (see Section 4.1).</b>  <b>Related commands:</b>  <table border="1" data-bbox="418 1486 1430 1726"> <tr> <td><b>clear aaa local user fail-attempts [username username   all]</b></td> <td><b>Clears the unsuccessful login attempts of the user.</b></td> </tr> <tr> <td><b>clear aaa local user lockout username [username]</b></td> <td><b>Unlocks the locked-out user.</b></td> </tr> <tr> <td><b>show aaa local user lockout</b></td> <td><b>Displays a list of all locked-out users.</b></td> </tr> </table> <b>Note: this lockout only applies to privilege 14 users and below.</b>  <b>Note: Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.</b>	<b>clear aaa local user fail-attempts [username username   all]</b>	<b>Clears the unsuccessful login attempts of the user.</b>	<b>clear aaa local user lockout username [username]</b>	<b>Unlocks the locked-out user.</b>	<b>show aaa local user lockout</b>	<b>Displays a list of all locked-out users.</b>
<b>clear aaa local user fail-attempts [username username   all]</b>	<b>Clears the unsuccessful login attempts of the user.</b>						
<b>clear aaa local user lockout username [username]</b>	<b>Unlocks the locked-out user.</b>						
<b>show aaa local user lockout</b>	<b>Displays a list of all locked-out users.</b>						

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.4 FIA\_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	The evaluator examined the section titled <b>User Lockout</b> in the AGD to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that:  <b>Note: this lockout only applies to privilege 14 users and below.</b>  <b>Note: Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 FIA\_PMG\_EXT.1

5.6.2.1 FIA\_PMG\_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of characters supported for administrator passwords.
Evaluator Findings	The evaluator examined the section titled <b>FIA_PMG_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of characters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that  <b>The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”). Minimum password length is settable by the Authorized Administrator, and supports passwords of 1 to 127 characters.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FIA\_PMG\_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it:  a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and  b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
-----------	--

Evaluator Findings	<p>The evaluator examined the section titled <b>Passwords</b> in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>To prevent administrators from choosing insecure passwords, each password must be:</b></p> <p><b>1. At least 15 characters long. Use the following command to set the minimum length to 15 or greater. Password length is configurable up to 127 characters.</b></p> <p><b>TOE-common-criteria (config)#security passwords min-length length</b></p> <p><b>Example: TOE-common-criteria (config)# security passwords min-length 15</b></p> <p><b>Note: Details for the security passwords min-length command can be found in the: [8] Under Reference Guides <a href="#">??</a>Command References <a href="#">??</a>Security and VPN <a href="#">??</a>See manual Cisco IOS Security Command Reference: Commands S to Z.</b></p> <p><b>2. Composed of any combination of characters that includes characters for at least 3 of these four character sets: upper case letters, lower case letters, numerals, and the following special characters: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, “)”. Configure the router to enforce that complexity requirement by using enabling “aaa password restriction”.</b></p> <p><b>Example: TOE-common-criteria (config)# aaa password restriction</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 5.6.3 FIA\_PSK\_EXT.1/MACsec

#### 5.6.3.1 FIA\_PSK\_EXT.1/MACsec TSS 1

Objective	<p>The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.</p>
Evaluator Findings	<p>The evaluator examined the <b>FIA_PSK_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE supports use of pre-shared keys for MACsec key agreement protocols. The pre-shared keys are not generated by the TOE but the TOE accepts the keys in the form of HEX strings. This is done via the CLI configuration command – “key chain test_key macsec.” The TOE accepts pre-shared keys of 32 and 64 characters in length only. The text-based pre-shared keys are conditioned by the prf function HMAC-SHA-1 configured by the administrator.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.3.2 FIA\_PSK\_EXT.1/MACsec Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported.
Evaluator Findings	<p>The evaluator examined the section titled <b>MACsec and MKA Configuration</b> in the AGD to verify that it provides guidance to administrators on the composition of strong pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in [16]:</b></p> <p><a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html</a></p> <p><b>Under Information About WAN MACsec and MKA Support Enhancements, in the section “Key Lifetime and Hitless Key Rollover” the appropriate guidance can be found. The evaluator found that the AGD provided instructions on configuring the TOE to accept bit-based keys, using the CLI and a note in the AGD that says:</b></p> <p><b>Note: MACsec supports pre-shared keys between of 32 and 64 characters in length only</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.3.3 FIA\_PSK\_EXT.1/MACsec Guidance 2

Objective	The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement or generating a bit-based pre-shared key (or both).
Evaluator Findings	<p>The evaluator examined the section titled <b>MACsec and MKA Configuration</b> in the AGD to verify that it contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement or generating a bit-based pre-shared key (or both). Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in [16]:</b></p> <p><a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html</a></p> <p><b>Under Information About WAN MACsec and MKA Support Enhancements, in the section “Key Lifetime and Hitless Key Rollover” the appropriate guidance can be found. The evaluator found that the AGD provided instructions on configuring the TOE to accept bit-based keys, using the CLI and a note in the AGD that says:</b></p> <p><b>Note: MACsec supports pre-shared keys between of 32 and 64 characters in length only</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass



5.6.4 FIA\_PSK\_EXT.1/VPN

5.6.4.1 FIA\_PSK\_EXT.1/VPN TSS 1

Objective	The evaluator shall examine the TSS to ensure that it identifies all protocols that allow both text-based and bit-based pre-shared keys, and states that text-based pre-shared keys of 22 characters are supported. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by the protocol, and that this conditioning is consistent with the last selection in the FIA_PSK_EXT.1.3 requirement.
Evaluator Findings	<p>The evaluator examined the <b>FIA_PSK_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies all protocols that allow both text-based and bit-based pre-shared keys, and states that text-based pre-shared keys of 22 characters are supported. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Through the implementation of the CLI, the TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. Preshared keys can be entered as ASCII character strings, or HEX values. The TOE supports keys that are from 22 characters in length up to 127 bytes in length and composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”). The data that is input is conditioned by the cryptographic module prior to use via SHA-1.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.4.2 FIA\_PSK\_EXT.1/VPN Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.
Evaluator Findings	<p>The evaluator examined the section titled <b>IKEv1 Transform Sets</b> and <b>IKEv2 Transform Sets</b> in the AGD to verify that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. Upon investigation, the evaluator found that both the AGD state that:</p> <p><b>TOE-common-criteria(config-isakmp)# Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4</b></p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”).</b></p> <p><b>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.</b></p>

	<p><b>TOE-common-criteria (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC</b></p> <p>This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.</p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “”).</b></p> <p>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, but longer keys increase processing time.</p> <p>HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: ‘pre-shared-key hex [hex key]’.</p> <p>For example: pre-shared-key hex 0x6A6B6C. See ‘pre-shared-key (IKEv2 keyring)’ in [8] for more information on this command.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.4.3 FIA\_PSK\_EXT.1/VPN Guidance 2

Objective	<p>The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1 in the Base-PP.</p>
Evaluator Findings	<p>The evaluator examined the sections titled <b>IKEv1 Transform Sets</b> and <b>IKEv2 Transform Sets</b> in the AGD to verify that it contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement or generating a bit-based pre-shared key (or both), and it describes the process by which the bit-based pre-shared keys are generated. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>TOE-common-criteria(config-isakmp)# Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4</b></p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “”).</b></p> <p>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.</p> <p><b>TOE-common-criteria (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC</b></p> <p>This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.</p> <p><b>Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “”).</b></p>

	<p>The TOE supports pre-shared keys up to 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, but longer keys increase processing time.</p> <p>HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: 'pre-shared-key hex [hex key]'.  For example: pre-shared-key hex 0x6A6B6C. See 'pre-shared-key (IKEv2 keyring)' in [8] for more information on this command</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.5 FIA\_UIA\_EXT.1

5.6.5.1 FIA\_UIA\_EXT.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>FIA_UIA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.</b></p> <p><b>The TOE provides a local password-based authentication mechanism as well as RADIUS AAA server for remote authentication.</b></p> <p><b>At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.5.2 FIA\_UIA\_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.
Evaluator Findings	<p>The evaluator examined the section titled <b>FIA_UIA_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.5.3 FIA\_UIA\_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	<p>The evaluator examined the following section in the AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD states that:</p> <ul style="list-style-type: none"> <li>• Initial Setup via Direct Console Connection</li> <li>• Administrator Configuration and Credentials</li> <li>• Remote Administration Protocols</li> <li>• Authentication Server Protocols</li> <li>• User Roles</li> <li>• Passwords</li> <li>• Identification and Authentication</li> </ul> <p>The evaluator found that each section in the AGD provides instruction for configuring user authentication on the TOE. Authentication may be configured via CLI. The instructions provided by the AGD place the TOE in a configuration that requires authentications for all administrative access.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.6 FIA\_UAU.7

5.6.6.1 FIA\_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	The evaluator examined the AGD and verified that no preparatory steps are required to ensure that authentication data is not revealed while entering the credentials.  It was found during testing that the TOE does not provide any feedback while entering the password at both the directly connected and remote login prompt.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7 FIA\_X509\_EXT.1/Rev

5.6.7.1 FIA\_X509\_EXT.1/Rev TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).
Evaluator Findings	The evaluator examined the section titled <b>FIA_X509_EXT.1/Rev</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that:  <b>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.</b>  <b>The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates.</b>  <b>CRL is configurable and may be used for certificate revocation. The authorized administrator could use the “revocation-check” command to specify at least one method of revocation checking; CRL is the default method and must be selected in the evaluated configuration as the ‘none’ option is not allowed. The authorized administrator sets the trust point and its name and the revocation-check method.</b>

	<p>The extendedKeyUsage field is validated according to the following rules:</p> <ul style="list-style-type: none"> <li>• Certificates used for trusted updates and executable code integrity verification have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3)</li> <li>• Server certificates have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field</li> <li>• Client certificates have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2)</li> <li>• OCSP certificates presented for OCSP responses have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.</li> </ul> <p>Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

5.6.7.2 FIA\_X509\_EXT.1/Rev TSS 2

Objective	The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.
Evaluator Findings	<p>The evaluator examined <b>FIA_X509_EXT.1/Rev</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>CRL is configurable and may be used for certificate revocation. The authorized administrator could use the “revocation-check” command to specify at least one method of revocation checking; CRL is the default method and must be selected in the evaluated configuration as the ‘none’ option is not allowed. The authorized administrator sets the trust point and its name and the revocation-check method.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.7.3 FIA\_X509\_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
-----------	--

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled <b>X.509 Certificates</b> in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.</b></p> <p><b>Creation of these certificates and loading them on the TOE is covered in [9], and a portion of the TOE configuration for use of these certificates follows below.</b></p> <p><b>Perform this task to set up the certificate revocation mechanism--CRLs--that is used to check the status of certificates in a PKI.</b></p> <p><b>Use the revocation-check command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.</b></p> <p style="text-align: center;"><b>(ca-trustpoint)#revocation-check crl</b></p> <p><b>If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.6.8 FIA\_X509\_EXT.2

5.6.8.1 FIA\_X509\_EXT.2 TSS 1

<p>Objective</p>	<p>The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the <b>FIA_X509_EXT.2</b> entry in section titled <b>TOE Summary Specification</b> Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.</b></p> <p><b>The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as:</b></p> <ul style="list-style-type: none"> <li>• alt-subject-name</li> <li>• expires-on</li> <li>• issuer-name</li> <li>• name</li> <li>• serial-number</li> <li>• subject-name</li> </ul>

	<ul style="list-style-type: none"> <li>• unstructured-subject-name</li> <li>• valid-start</li> </ul> <p>This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for one IPsec connection, while another certificate from another CA could be used for a different IPsec connection. However, the default configuration is a single certificate from one CA that is used for all authenticated connections.</p> <p>The certificate chain path validation is configured on the TOE by first setting crypto pki trustpoint name and then configuring the level to which a certificate chain is processed on all certificates including subordinate CA certificates using the chain-validation command. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.8.2 FIA\_X509\_EXT.2 TSS 2

Objective	<p>The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.</p>
Evaluator Findings	<p>The evaluator examined the <b>FIA_X509_EXT.2</b> entry in section titled <b>TOE Summary Specification</b> the Security Target to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>CRL is configurable and may be used for certificate revocation. The authorized administrator could use the “revocation-check” command to specify at least one method of revocation checking; CRL is the default method and must be selected in the evaluated configuration as the ‘none’ option is not allowed. The authorized administer sets the trust point and its name and the revocation-check method.</b></p> <p>The certificate chain path validation is configured on the TOE by first setting crypto pki trustpoint name and then configuring the level to which a certificate chain is processed on all certificates including subordinate CA certificates using the chain-validation command. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.</p> <p>Next, the evaluator examined the section titled <b>Configuring a Revocation Mechanism for PKI Certificate Status Checking</b> in the AGD to verify that it describes the expected behavior of the TOE when the validity of peer certificates cannot be determined. Upon investigation, the evaluator found that the AGD states that:</p>



	<p>Use the revocation-check command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.</p> <p><b>(ca-trustpoint)#revocation-check crl</b></p> <p>If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.8.3 FIA\_X509\_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	<p>The evaluator examined the section titled <b>X.509 Certificates</b> in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.</b></p> <p><b>Creation of these certificates and loading them on the TOE is covered in [9], and a portion of the TOE configuration for use of these certificates follows below.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.8.4 FIA\_X509\_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	<p>The evaluator examined the section titled <b>Configuring a Revocation Mechanism for PKI Certificate Status Checking</b> in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Use the revocation-check command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.</b></p> <p><b>(ca-trustpoint)#revocation-check crl</b></p>

	<p><b>If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6.8.5 FIA\_X509\_EXT.2 Guidance 3

Objective	<p>The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>X.509 Certificates and Configuring a Revocation Mechanism for PKI Certificate Status Checking</b> in the AGD. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.</b></p> <p><b>Creation of these certificates and loading them on the TOE is covered in [9], and a portion of the TOE configuration for use of these certificates follows below.</b></p> <p><b>The evaluator observed the subsequent steps and found that the AGD included all the steps for configuring the operating environment. Further the AGD states that,</b></p> <p><b>Use the revocation-check command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.</b></p> <p style="text-align: center;"><b>(ca-trustpoint)#revocation-check crl</b></p> <p><b>If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass.

5.6.9 FIA\_X509\_EXT.3

5.6.9.1 FIA\_X509\_EXT.3 TSS 1

Objective	<p>If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.</p>
Evaluator Findings	<p>The evaluator examined the <b>FIA_X509_EXT.3</b> SFR in the ST and verified that "device-specific information" is not selected. Therefore, this assurance activity is not applicable.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.9.2 FIA\_X509\_EXT.3 Guidance 1

Objective	The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.
Evaluator Findings	The evaluator examined the section titled <b>Creation of the Certificate Signing Request</b> in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD states that:  <b>All of the certificates include at least the following information:</b>  <b>public key and (Common Name, Organization, Organizational Unit, Country) &lt;subject-name&gt; CN=catTOE.cisco.com,O=cisco,OU=TAC,C=U</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

## 5.7 TSS and Guidance Activities (Security Management)

5.7.1 FMT\_MOF.1/ManualUpdate

5.7.1.1 FMT\_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined the <b>OE. UPDATES</b> entry in section titled <b>Security Measures for the Operational Environment</b> and <b>Product Updates</b> in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states that:  <b>The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</b>  The evaluator examined the section titled Product Updates in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that:  Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See Section 2, steps 7 and 9 above for the method to download and verify an image prior to running it on the TOE.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FMT\_FMT\_MOF.1/Functions

5.7.2.1 FMT\_MOF.1/Functions TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).
Evaluator Findings	<p>The evaluator examined the <b>FMT_MOF.1/Functions</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.2.2 FMT\_MOF.1/Functions Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.
Evaluator Findings	<p>The evaluator examined the section titled <b>Logging Protection</b> in the AGD to verify that it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>If an authorized administrator wants to backup the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:</b></p> <ol style="list-style-type: none"> <li><b>1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or</b></li> <li><b>2. With a syslog server is not directly co-located with the TOE, but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.</b></li> </ol> <p><b>When a Syslog server is configured on the TOE, generated audit events are simultaneously sent to the external server and the local logging buffer</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### 5.7.3 FMT\_MOF.1/Services

#### 5.7.3.1 FMT\_MOF.1/Services TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the <b>FMT_MOF.1/Services</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the TSS states that:  <b>See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.7.3.2 FMT\_MOF.1/Services Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the section titled <b>Secure Acceptance of the TOE</b> in the AGD to verify that it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the AGD states that:  <b>Start your router as described in [13] and executing associated commands in [8] and [12]. Confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### 5.7.4 FMT\_MTD.1/CoreData

#### 5.7.4.1 FMT\_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	The evaluator examined the <b>FMT_MTD.1/CoreData</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies administrative functions

	<p>that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable.</b></p> <p>The evaluator examined <b>FMT_MTD.1/CoreData</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The term “Security Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege. No administrative functionality is available prior to administrative login.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.4.2 FMT\_MTD.1/CoreData TSS 2

Objective	<p>If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE’s trust store is restricted.</p>
Evaluator Findings	<p>The evaluator examined the <b>FIA_X509_EXT.1/Rev</b> and <b>FMT_MTD.1/CoreData</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE’s trust store is restricted. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the router and the certificates from being tampered with or deleted. Only authorized administrators with the necessary privilege level can access the certificate storage and add/delete them. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE.</b></p> <p><b>The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data.</b></p>

	<p><b>See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.4.3 FMT\_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.
Evaluator Findings	<p>The evaluator examined the following sections in the AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD includes configuration of the following in the respective sections,</p> <ul style="list-style-type: none"> <li>• <b>Audit Configuration</b> <ul style="list-style-type: none"> <li>○ <i>Sections titled 'Logging Configuration', 'Logging Protection', and 'Security Relevant Events'</i></li> </ul> </li> <li>• <b>Identification/Authentication</b> <ul style="list-style-type: none"> <li>○ <i>Sections titled 'User Roles', 'Passwords', 'Identification and Authentication', 'User Lockout' and 'Authentication Server Protocols'</i></li> </ul> </li> <li>• <b>SSH configuration</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'Remote Administration Protocols'</i></li> </ul> </li> <li>• <b>IPsec configuration</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'IPsec Overview'</i></li> </ul> </li> <li>• <b>Time stamps</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'Clock Management'</i></li> </ul> </li> <li>• <b>Session time-out</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'Session Termination'</i></li> </ul> </li> <li>• <b>TOE Banner</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'Login Banners'</i></li> </ul> </li> <li>• <b>TOE updates</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'Secure Acceptance of the TOE' and 'Product Updates'</i></li> </ul> </li> <li>• <b>X.509 Certificates</b> <ul style="list-style-type: none"> <li>○ <i>Section titled 'X.509 Certificates'</i></li> </ul> </li> </ul> <p>The evaluator found that this encompasses all the TSF-data manipulating functionality required by the NDcPP.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.4.4 FMT\_MTD.1/CoreData Guidance 2

Objective	If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE
-----------	---

	supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.
Evaluator Findings	<p>The evaluator examined the section titled <b>Storing Certificates to a Local Storage Location</b> in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD states that :</p> <p><b>Certificates are stored to NVRAM by default; however, some routers do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates.</b></p> <p>The evaluator examined the section titled <b>Storing Certificates to a Local Storage Location</b> in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states that</p> <p><b>How to Specify a Local Storage Location for Certificates -</b>  <b>The summary steps for storing certificates locally to the TOE are as follows:</b>  <b>Enter configure terminal mode:</b>  <b>TOE-common-criteria# configure terminal</b></p> <p><b>Specify the local storage location for certificates: crypto pki certificate storage location-name</b>  <b>Device(config)# crypto pki certificate storage bootflash:/certs</b></p> <p><b>Exit: Device(config)# exit</b></p> <p><b>Save the changes made:</b>  <b>Device# copy system:running-config nvram:startup-config</b></p> <p><b>Display the current setting for the PKI certificate storage location:</b>  <b>Device# show crypto pki certificates storage</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.5 FMT\_MTD.1/CryptoKeys

5.7.5.1 FMT\_MTD.1/CryptoKeys TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
-----------	--



<p>Evaluator Findings</p>	<p>The evaluator examined the section titled <b>FCS_CKM.1, FCS_CKM.4</b> and <b>FMT_MTD.1/CryptoKeys</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that :</p> <p><b>The TOE implements DH group 14 key establishment schemes that NIST Special Publication 800-56A Revision 3 and RFC 3526. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes.</b></p> <p><b>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6.</b></p> <p><b>Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes and Appendix B.4 for ECDSA schemes.</b></p> <p><b>The TOE can create an RSA public-private key pair, with a minimum RSA key size of 3072-bit and ECDSA key pairs using NIST curves P-256 and P-384. Both RSA and ECC schemes can be used to generate a Certificate Signing Request (CSR).</b></p> <p><b>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). Refer to Table 18 for more information on the key zeroization.</b></p> <p><b>See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI.</b></p> <p><b>The Security Administrator is able to manage the cryptographic keys (generating keys, importing keys, or deleting keys) that are used in IPsec, MACSEC, and SSH communications. These keys can be managed via CLI as part of following operations:</b></p> <ul style="list-style-type: none"> <li>• <b>SSH session keys– as part of session establishment and termination</b></li> <li>• <b>SSH public/private keys – generate keypair, import/export public keys, public key-based authentication</b></li> <li>• <b>MACsec keys – as part of MACsec session establishment and termination</b></li> <li>• <b>Zeroize – delete keys</b></li> </ul> <p>The evaluator examined the FMT_SMF.1 TSS and found that it includes the options for cryptographic keys</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.7.5.2 FMT\_MTD.1/CryptoKeys Guidance 2

<p>Objective</p>	<p>For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.</p>
------------------	---

Evaluator Findings	<p>The evaluator examined the section titled <b>Generate a Key Pair</b> in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>RSA and ECDSA keys are generated in pairs—one public key and one private key:</b></p> <p><b>(config)# crypto key generate rsa modulus 3072</b></p> <p>- or -</p> <p><b>(config)# crypto key generate ec keysizes &lt;256   384&gt; exportable</b></p> <p>The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.</p> <p><b>Note: Only one set of keys can be configured using the crypto key generate command at a time. Repeating the command overwrites the old keys.</b></p> <p><b>Note: If the configuration is not saved to NVRAM with a “copy run start”, the generated keys are lost on the next reload of the router.</b></p> <p><b>Note: If the error “% Please define a domain-name first” is received, enter the command ‘ip domain-name [domain name].</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.6 FMT\_SMF.1

5.7.6.1 FMT\_SMF.1 TSS 1

Objective	<p>The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).</p> <p>The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.</p> <p>MACsec:</p> <p>The evaluator shall verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP.</p>
Evaluator Findings	<p>The evaluator examined the <b>FMT_SMF.1</b> entry in section titled <b>TOE Summary Specification</b> in the TSS to verify that it details which security management functions are available through which interface(s). The evaluator examined the following sections in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator mentioned the respective sections in AGD for the points stated in the TSS as below:</p> <p><b>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include –</b></p> <ul style="list-style-type: none"> <li>• <b>Ability to administer the TOE locally and remotely;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘Initial Setup via Direct Console Connection’</i></li> </ul> </li> </ul>

- *Section 'Remote Administration Protocols'*
- **Ability to configure the access banner;**
  - *Section 'Login Banners'*
- **Ability to configure the session inactivity time before session termination or locking;**
  - *Section 'Session Termination'*
- **Ability to update the TOE, and to verify the updates using digital signature and [hash comparison] capability prior to installing those updates;**
  - *Section 'Secure Acceptance of the TOE'*
  - *Section 'Product Updates'*
- **Ability to configure the authentication failure parameters for FIA\_AFL.1;**
  - *Section 'User Lockout'*
- **Ability to manage the cryptographic keys;**
  - *Section 'Remote Administration Protocols'*
- **Ability to configure the cryptographic functionality;**
  - *Section 'Remote Administration Protocols'*
- **Ability to configure the lifetime for IPsec SAs;**
  - *Section 'Virtual Private Networks'*
- **Ability to import X.509v3 certificates to the TOE's trust store;**
  - *Section 'X.509 Certificates'*
- **Ability of a Security Administrator to Generate a PSK-based CAK and install it in the device.**
  - *Section 'MACsec and MKA Configuration'*
- **Ability of a Security Administrator to Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA());**
  - *Section 'MACsec and MKA Configuration'*
- **Ability of a Security Administrator to Specify a lifetime of a CAK**
  - *Section 'MACsec and MKA Configuration'*
- **Ability of a Security Administrator to Enable, disable, or delete a PSK-based CAK using [[CLI management commands]]**
  - *Section 'MACsec and MKA Configuration'*
- **Ability of a Security Administrator to Configure the number of failed administrator authentication attempts that will cause an account to be locked out**
  - *Section 'User Lockout'*
- **Ability to start and stop services;**
  - *Section 'Initial Setup via Direct Console Connection'*
- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.**
  - *Section 'X.509 Certificates'*
- **Ability to configure the reference identifier for the peer;**
  - *Section 'Configure Reference Identifier'*
- **Ability to set the time which is used for time-stamps;**
  - *Section 'Clock Management'*
- **Ability to re-enable an Administrator account;**
  - *Section 'User Lockout'*

	<ul style="list-style-type: none"> <li>• <b>Ability to modify the behaviour of the transmission of audit data to an external IT entity;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Logging Configuration'</i></li> </ul> </li> <li>• <b>Ability to manage the trusted public keys database;</b> <ul style="list-style-type: none"> <li>○ <i>Section Configuring Certificate Chain Validation.</i></li> </ul> </li> </ul> <p>All functions are available via local and remote CLI. The AGD describes the local interface in the sections titled <b>Supported non-TOE Hardware/Software/Firmware</b> and <b>Initial Setup via Direct Console Connection</b>.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.6.2 FMT\_SMF.1 TSS 2

Objective	<p>The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).</p> <p>The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.</p> <p>MACsec:</p> <p>The evaluator shall verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP.</p>
Evaluator Findings	<p>The evaluator examined the <b>FMT_SMF.1</b> entry in section titled <b>TOE Summary Specification</b> in the TSS to verify that it details which security management functions are available through which interface(s). The evaluator examined the following sections in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator mentioned the respective sections in AGD for the points stated in the TSS as below:</p> <p><b>Information about TSF-initiated Termination is covered in the TSS under FTA_SSL_EXT.1 or FTA_SSL.3.</b></p> <p>In addition to the above, the TSS directs the reader to the FTA_SSL_EXT.1 or FTA_SSL.3 TSS entries for information on managing TSF-initiated termination. The management guidance for these SFRs is provided in the appropriate FTA_SSL_EXT.1 and FTA_SSL.3 assurance activities.</p> <p>All functions are available via local and remote CLI. The AGD describes the local interface in the sections titled <b>Supported non-TOE Hardware/Software/Firmware</b> and <b>Initial Setup via Direct Console Connection</b>.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

Objective	<p>The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.</p> <p>MACsec:</p> <p>The evaluator shall examine the operational guidance to determine that it provides instructions on how to perform each of the management functions defined in this SFR in addition to those required by the base NDcPP.</p>
Evaluator Findings	<p>The evaluator examined the following sections in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator mentioned the respective sections in the AGD for the points stated in the SFR as below:</p> <p><b>The specific management capabilities available from the TOE include:</b></p> <ul style="list-style-type: none"> <li>• <b>Ability to administer the TOE locally and remotely;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Initial Setup via Direct Console Connection'</i></li> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>• <b>Ability to configure the access banner;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Login Banners'</i></li> </ul> </li> <li>• <b>Ability to configure the session inactivity time before session termination or locking;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Session Termination'</i></li> </ul> </li> <li>• <b>Ability to update the TOE, and to verify the updates using digital signature and <u>[hash comparison]</u> capability prior to installing those updates;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Secure Acceptance of the TOE'</i></li> <li>○ <i>Section 'Product Updates'</i></li> </ul> </li> <li>• <b>Ability to configure the authentication failure parameters for FIA_AFL.1;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'User Lockout'</i></li> </ul> </li> <li>• <b>Ability to manage the cryptographic keys;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>• <b>Ability to configure the cryptographic functionality;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Remote Administration Protocols'</i></li> </ul> </li> <li>• <b>Ability to configure the lifetime for IPsec SAs;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Virtual Private Networks'</i></li> </ul> </li> <li>• <b>Ability to import X.509v3 certificates to the TOE's trust store;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'X.509 Certificates'</i></li> </ul> </li> <li>• <b>Ability of a Security Administrator to Generate a PSK-based CAK and install it in the device.</b> <ul style="list-style-type: none"> <li>○ <i>Section 'MACsec and MKA Configuration'</i></li> </ul> </li> <li>• <b>Ability of a Security Administrator to Manage the Key Server to create, delete, and activate MKA participants <u>[as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry)]</u> and section. 12.2 (cf. function <u>createMKA()</u>);</b> <ul style="list-style-type: none"> <li>○ <i>Section 'MACsec and MKA Configuration'</i></li> </ul> </li> <li>• <b>Ability of a Security Administrator to Specify a lifetime of a CAK</b> <ul style="list-style-type: none"> <li>○ <i>Section 'MACsec and MKA Configuration'</i></li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Ability of a Security Administrator to Enable, disable, or delete a PSK-based CAK using <u>[[CLI management commands]]</u></b> <ul style="list-style-type: none"> <li>○ <i>Section ‘MACsec and MKA Configuration’</i></li> </ul> </li> <li>• <b>Ability of a Security Administrator to Configure the number of failed administrator authentication attempts that will cause an account to be locked out</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘User Lockout’</i></li> </ul> </li> <li>• <b>Ability to start and stop services;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘Initial Setup via Direct Console Connection’</i></li> </ul> </li> <li>• <b>Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘X.509 Certificates’</i></li> </ul> </li> <li>• <b>Ability to configure the reference identifier for the peer;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘Configure Reference Identifier’</i></li> </ul> </li> <li>• <b>Ability to set the time which is used for time-stamps;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘Clock Management’</i></li> </ul> </li> <li>• <b>Ability to re-enable an Administrator account;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘User Lockout’</i></li> </ul> </li> <li>• <b>Ability to modify the behaviour of the transmission of audit data to an external IT entity;</b> <ul style="list-style-type: none"> <li>○ <i>Section ‘Logging Configuration’</i></li> </ul> </li> <li>• <b>Ability to manage the trusted public keys database;</b> <ul style="list-style-type: none"> <li>○ <i>Section Configuring Certificate Chain Validation</i></li> </ul> </li> </ul> <p>The evaluator examined the section titled <b>Login Banners</b> in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states that</p> <p><b>The TOE may be configured by the privileged administrators with banners using the banner login command. This banner is displayed before the username and password prompts. To create a banner of text “This is a banner” use the command</b></p> <p><b>banner login d This is a banner d</b></p> <p><b>where d is the delimiting character. The delimiting character may be any character except ‘?’, and it must not be part of the banner message.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1 FMT\_SMF.1/VPN

5.7.1.1 FMT\_SMF.1/VPN TSS

Objective	The evaluator shall examine the TSS to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the TSS identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Evaluator Findings	The evaluator examined the <b>FMT_SMF.1/VPN</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS states that all management

	<p>functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that the TSS states:</p> <p><b>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include -</b></p> <ul style="list-style-type: none"> <li>• <b>The ability to define packet filtering rules;</b></li> <li>• <b>The ability to associate packet filtering rules to network interfaces;</b></li> <li>• <b>The ability to order packet filtering rules by priority;</b></li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.7.1.2 FMT\_SMF.1/VPN Guidance

Objective	<p>The evaluator shall examine the operational guidance to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the operational guidance identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.</p>
Evaluator Findings	<p>The evaluator examined the section in <b>Base Firewall Rule Set Configuration</b> in the AGD to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that following points in TSS are present in the AGD:</p> <ul style="list-style-type: none"> <li>• <b>Ability to define packet filtering rules;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Base Firewall Rule Set Configuration'</i></li> </ul> </li> <li>• <b>Ability to associate packet filtering rules to network interfaces;</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Base Firewall Rule Set Configuration'</i></li> </ul> </li> <li>• <b>Ability to order packet filtering rules by priority</b> <ul style="list-style-type: none"> <li>○ <i>Section 'Base Firewall Rule Set Configuration'</i></li> </ul> </li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.7.1.3 FMT\_SMF.1 Guidance 1

Objective	<p>The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.</p>
Evaluator Findings	<p>The evaluator examined the section titled 'Initial Setup via Direct Console Connection' in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD describes the initial configuration of the TOE through the local interface.</p> <p>The evaluator examined the section titled 'Identification and Authentication' in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states that an administrator can</p>

	connect to the TOE locally through a direct console connection or remotely via SSHv2 or a RADIUS authentication server connected securely through IPsec.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FMT\_SMR.2

5.7.2.1 FMT\_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
Evaluator Findings	<p>The evaluator examined the <b>FMT_SMR.2</b> entry in section titled <b>TOE Summary Specification</b> in the TSS to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. Note: the levels are not hierarchical.</b></p> <p><b>The term “Security Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.</b></p> <p><b>The privilege level determines the functions the user can perform; hence the Security Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS-XE Command Reference Guide for available commands and associated roles and privilege levels.</b></p> <p><b>The TOE can and shall be configured to authenticate all access to the command line interface using a username and password.</b></p> <p><b>The TOE supports both local administration via a directly connected console cable and remote administration via SSH or IPsec over SSH.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.2.2 FMT\_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	The evaluator examined the section titled <b>Initial Setup via Direct Console Connection and Remote Administration Protocols</b> in the AGD to verify that it contains instructions for



	<p>administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD states that</p> <p><b>To login to the router, connect via SSH or local console. Enter the username and password when prompted.</b></p> <p><b>User Access Verification</b></p> <p><b>Username: &lt;enter configured username&gt;</b></p> <p><b>Password: &lt;enter configured password&gt;</b></p> <p>The evaluator found that the AGD describes the configuration necessary to administer the TOE using the CLI from the following interfaces:</p> <ol style="list-style-type: none"> <li>1. Via Direct console connection – Section <b>Initial Setup via Direct Console Connection</b></li> <li>2. Via Remote connection using SSH – Section <b>Remote Administration Protocols</b></li> </ol> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 5.8 TSS and Guidance Activities (Packet Filtering)

### 5.8.1 FPF\_RUL\_EXT.1

#### 5.8.1.1 FPF\_RUL\_EXT.1.1 TSS 1

Objective	<p>The evaluator shall verify that the TSS provide a description of the TOE’s initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process.</p> <p>The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.</p>
Evaluator Findings	<p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS provides a description of the TOE’s initialization/startup process and a discussion that supports the assertion that packets cannot flow during this process. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/startup that the access lists are not enforced on an interface. The initialization process first initializes the operating system, and then the</b></p>

	<p>networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational.</p> <p>During initialization/startup (while the TOE is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the TOE interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the TOE will reload without forwarding traffic. If a critical component of the TOE, such as the clock or cryptographic modules, fails while the TOE is in an operational state, the TOE will reload, which stops the flow of traffic.</p> <p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS includes a narrative that identifies the components involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). This is the default action that occurs on an interface if no ACL rule is found. If a packet arrives that does not meet any rule, it is expected to be dropped. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.1.2 FPF\_RUL\_EXT.1.1 Guidance 1

Objective	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
Evaluator Findings	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
Verdict	Pass

5.8.1.3 FPF\_RUL\_EXT.1.4 TSS 1

Objective	<p>The evaluator shall verify that the TSS describes a Packet Filtering policy that can use the following fields for each identified protocol, and that the RFCs identified for each protocol are supported:</p> <ul style="list-style-type: none"> <li>• IPv4 (RFC 791) <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Protocol</li> </ul> </li> <li>• IPv6 (RFC 2460) <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Next Header (Protocol)</li> </ul> </li> <li>• TCP (RFC 793) <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> </ul>
-----------	--

	<ul style="list-style-type: none"> <li>• UDP (RFC768) <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> </ul> <p>The evaluator shall verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing).</p> <p>The evaluator shall verify that each rule can identify the following actions: permit, discard, and log.</p> <p>The evaluator shall verify that the TSS identifies all interface types subject to the Packet Filtering policy and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes a Packet Filtering policy, describes how conformance with the identified RFCs has been determined, each rule can identify the required actions, identifies all interface types subject to the Packet Filtering policy and explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using access and crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. The access lists can be applied to all the network interfaces.</b></p> <p><b>The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.</b></p> <p><b>By implementing rules that defines the permitted flow of traffic between interfaces of the TOE for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on:</b></p> <ol style="list-style-type: none"> <li>1. presumed address of source</li> <li>2. presumed address of destination</li> <li>3. transport layer protocol (or next header in IPv6)</li> <li>4. Service used (UDP or TCP ports, both source and destination)</li> <li>5. Network interface on which the connection request occurs</li> </ol> <p><b>These rules are supported for the following protocols: RFC 791(IPv4); RFC 2460 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing.</b></p> <p>The TSS also states:</p> <p><b>These rules are entered in the form of access lists at the CLI (via 'access list' and 'access group' commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network;</b></p>

	<p>These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network;</p> <p>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network;</p> <p>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network;</p> <p>These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination.</p> <p>Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic through another network interface corresponding to the traffic's destination address.</p> <p>These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/startup that the access lists are not enforced on an interface. The initialization process first initializes the operating system, and then the networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.1.4 FPF\_RUL\_EXT.1.4 Guidance 1

Objective	<p>The evaluators shall verify that the operational guidance identifies the following protocols as being supported and the following attributes as being configurable within Packet filtering rules for the associated protocols:</p> <ul style="list-style-type: none"> <li>• IPv4 (RFC 791) <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Protocol</li> </ul> </li> <li>• IPv6 (RFC 2460) <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Next Header (Protocol)</li> </ul> </li> <li>• TCP (RFC 793) <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> <li>• UDP (RFC768) <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> </ul> <p>The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, discard, and log.</p> <p>The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces.</p>
-----------	---

	<p>The guidance may describe the other protocols contained within the ST (e.g., IPsec, IKE, potentially HTTPS, SSH, and TLS) that are processed by the TOE. The evaluator shall ensure that it is made clear what protocols were not considered as part of the TOE evaluation.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled <b>Base Firewall Rule Set Configuration</b> in the AGD to verify that it identifies the required protocols as being supported and the required attributes as being configurable within Packet filtering rules, indicates that each rule can identify the required actions, explains how rules are associated with distinct network interfaces, and makes clear what protocols were not considered as part of the TOE evaluation. Upon investigation, the evaluator found that the AGD states that</p> <p><b>The PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW) contains requirements for the TOE basic packet filtering. Packet filtering is able to be done on many protocols by the TOE, including but not limited to (although the evaluation only covers IPv4, IPv6, TCP and UDP):</b></p> <ul style="list-style-type: none"> <li>• <b>IPv4 (RFC 791)</b></li> <li>• <b>IPv6 (RFC 2460)</b></li> <li>• <b>TCP (RFC 793)</b></li> <li>• <b>UDP (RFC 768)</b></li> <li>• <b>IKEv1 (RFCs 2407, 2408, 2409, RFC4109)</b></li> <li>• <b>IKEv2 (RFC 5996)</b></li> <li>• <b>IPsec ESP (RFCs 4301, 4303)</b></li> <li>• <b>SSH (RFCs 4251, 4252, 4253, 4254, 8308 section 3.1, 8332)</b></li> </ul> <p><b>The following attributes, at a minimum, are configurable within Packet filtering rules for the associated protocols:</b></p> <ul style="list-style-type: none"> <li>• <b>IPv4</b> <ul style="list-style-type: none"> <li>○ <b>Source address</b></li> <li>○ <b>Destination Address</b></li> <li>○ <b>Protocol</b></li> </ul> </li> <li>• <b>IPv6</b> <ul style="list-style-type: none"> <li>○ <b>Source address</b></li> <li>○ <b>Destination Address</b></li> <li>○ <b>Next Header (Protocol)</b></li> </ul> </li> <li>• <b>TCP</b> <ul style="list-style-type: none"> <li>○ <b>Source Port</b></li> <li>○ <b>Destination Port</b></li> </ul> </li> <li>• <b>UDP</b> <ul style="list-style-type: none"> <li>○ <b>Source Port</b></li> <li>○ <b>Destination Port</b></li> </ul> </li> </ul>

	<p>The evaluator found that the rules for packet filtering was mentioned in the section of the AGD.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.8.1.5 FPF\_RUL\_EXT.1.5 TSS 1

Objective	<p>The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.</p>
Evaluator Findings	<p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using access and crypto map sets. Therefore, traffic may be selected on the basis of the source and destination address, and optionally the Layer 4 protocol and port. The access lists can be applied to all the network interfaces.</b></p> <p><b>The TOE enforces information flow policies on network packets that are received by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.</b></p> <p><b>The TOE is capable of inspecting network packet header fields to determine if a packet is part of an established session or not. ACL rules still apply to packets that are part of an ongoing session.</b></p> <p><b>Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). This is the default action that occurs on an interface if no ACL rule is found. If a packet arrives that does not meet any rule, it is expected to be dropped. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied.</b></p> <p><b>These rules are entered in the form of access lists at the CLI (via ‘access list’ and ‘access group’ commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network;</b></p> <p><b>These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network;</b></p> <p><b>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network;</b></p> <p><b>These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network;</b></p> <p><b>These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination.</b></p>

	<p>Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic through another network interface corresponding to the traffic's destination address.</p> <p>These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/ startup that the access lists are not enforced on an interface. The initialization process first initializes the operating system, and then the networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.8.1.6 FPF\_RUL\_EXT.1.5 Guidance 1

Objective	The evaluator shall verify that the operational guidance describes how the order of Packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.
Evaluator Findings	<p>The evaluator examined the section titled <b>Base Firewall Rule Set Configuration</b> in the AGD to verify that it describes how the order of Packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Traffic matching is done based on a top-down approach in the access list. The first entry that a packet matches will be the one applied to it. The MOD_VPNGW requires that the TOE Access control lists (ACLs) are to be configured to drop all packet flows as the default rule and that traffic matching the acl be able to be logged. The drop all default rule can be achieved by including an ACL rule to drop all packets as the last rule in the ACL configuration. The logging of matching traffic is done by appending the key word "log-input" per the command reference at the end of the acl statements, as done below.</b></p> <p><b>Access lists must be configured on the TOE to meet the requirements of the MOD_VPNGW.</b></p> <p>The evaluator found that the AGD states that:</p> <p><b>A privileged authorized administrator may manipulate the ACLs using the commands ip inspect, access-list, crypto map, and access-group as described [8].</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.8.1.7 FPF\_RUL\_EXT.1.6 TSS 1 [TD0597]

Objective	The evaluator shall verify that the TSS describes the process for applying Packet Filtering rules and also that the behavior (either by default, or as configured by the administrator) is to discard packets when there is no rule match. <b>The evaluator shall verify the TSS describes when the IPv4/IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table.</b>
Evaluator Findings	<p>The evaluator examined the <b>FPF_RUL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the process for applying Packet filtering rules and that the behavior is to deny packets when there is no rule match. The evaluator also verified the TSS describes when the IPv4/IPv6 protocols supported by the</p>

TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table. Upon investigation, the evaluator found that the TSS states that:

**By implementing rules that defines the permitted flow of traffic between interfaces of the TOE for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on:**

1. presumed address of source
2. presumed address of destination
3. transport layer protocol (or next header in IPv6)
4. Service used (UDP or TCP ports, both source and destination)
5. Network interface on which the connection request occurs

These rules are supported for the following protocols: RFC 791(IPv4); RFC 2460 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing.

The following protocols are not supported and will be dropped before the packet is matched to an ACL; therefore, any “permit” or “deny” entries in an ACL will not show matches in the output of the ‘show ip access-list’ command.

- IPv4 - Protocol 2 (IGMP)  
Protocol 2 is configuration dependent and is not supported when the device is not participating in an IGMP routing group.
- IPv6 - Protocols 43 (IPv6-Route), 44 (IPv6-Frag), 51 (AH), 60 (IPv6-Opts), 135 (Mobility Header)

The TOE is capable of inspecting network packet header fields to determine if a packet is part of an established session or not. ACL rules still apply to packets that are part of an ongoing session.

Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). This is the default action that occurs on an interface if no ACL rule is found. If a packet arrives that does not meet any rule, it is expected to be dropped. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied.

These rules are entered in the form of access lists at the CLI (via ‘access list’ and ‘access group’ commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network;

These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network;

These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network;

These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network;

These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination.

Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic through another network interface corresponding to the traffic’s destination address.



	<p>These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/ startup that the access lists are not enforced on an interface. The initialization process first initializes the operating system, and then the networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.1.8 FPF\_RUL\_EXT.1.6 Guidance 1 [TD0597]

Objective	<p>The evaluator shall verify that the operational guidance describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the operational guidance provides the appropriate instructions to configure the behavior to discard packets with no matching rules. <b>The evaluator shall verify that the operational guidance describes the range of IPv4/IPv6 protocols supported by the TOE.</b></p>
Evaluator Findings	<p>The evaluator examined the section titled <b>Base Firewall Rule Set Configuration</b> in each AGD to verify that it describes the behavior if no rules or special conditions apply to the network traffic. The evaluator shall verify that the operational guidance describes the range of IPv4/IPv6 protocols supported by the TOE. Upon investigation, the evaluator found that both the AGDs state that:</p> <p><b>The following protocols are not supported and will be dropped before the packet is matched to an ACL; therefore, any “permit” or “deny” entries in an ACL will not show matches in the output of the ‘show ip access-list’ command.</b></p> <ul style="list-style-type: none"> <li>• <b>IPv4 - Protocol 2 (IGMP)</b> Protocol 2 is configuration dependent and is not supported when the device is not participating in an IGMP routing group.</li> <li>• <b>IPv6 - Protocols 43 (IPv6-Route), 44 (IPv6-Frag), 51 (AH), 60 (IPv6-Opts), 135 (Mobility Header)</b></li> </ul> <p>Traffic matching is done based on a top-down approach in the access list. The first entry that a packet matches will be the one applied to it. The MOD_VPNGW requires that the TOE Access control lists (ACLs) are to be configured to drop all packet flows as the default rule and that traffic matching the acl be able to be logged. The drop all default rule can be achieved by including an ACL rule to drop all packets as the last rule in the ACL configuration. The logging of matching traffic is done by appending the key word “log-input” per the command reference at the end of the acl statements, as done below.</p> <p><b>Access lists must be configured on the TOE to meet the requirements of the MOD_VPNGW.</b></p> <p><b>Note: These access lists must be integrated with the defined security policy for your TOE router. Enabling just these access lists with no permits will result in traffic being dropped. Ensure that your access list entries are inserted above the default deny acl.</b></p> <p>The evaluator found that the AGD states that:</p> <p><b>A privileged authorized administrator may manipulate the ACLs using the commands ip inspect, access-list, crypto map, and access-group as described [8].</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

## 5.9 TSS and Guidance Activities (Protection of the TSF)

### 5.9.1 FPT\_APW\_EXT.1

#### 5.9.1.1 FPT\_APW\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.
Evaluator Findings	<p>The evaluator examined <b>FPT_APW_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The password is encrypted by using the command "password encryption aes" used in global configuration mode. The "password encryption aes" command enables the functionality and the "key config-key password-encrypt" command is used to set the master password to be used to encrypt the preshared keys.</b></p> <p><b>The command service password-encryption applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords.</b></p> <p><b>Additionally, enabling the 'hidekeys' command in the logging configuration ensures that and passwords are not displayed in plaintext.</b></p> <p><b>The TOE includes a Master Passphrase feature that can be used to configure the TOE to encrypt all locally defined user passwords using AES. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. Password encryption is configured using the 'service password-encryption' command. There are no administrative interfaces available that allow passwords to be viewed as they are encrypted via the password-encryption service.</b></p> <p>The evaluator also examined the section titled <b>FIA_UAU.7</b> in the Security Target to verify that the TSS details that password are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that:</p>

	<p><b>When a user enters their password at the local console, the TOE displays no characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.2 FPT\_SKP\_EXT.1

5.9.2.1 FPT\_SKP\_EXT.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.</p>
Evaluator Findings	<p>The evaluator examined the <b>FPT_SKP_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE stores all private keys in a secure directory protected from access as there is no interface in which the keys can be accessed.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.3 FPT\_STM\_EXT.1

5.9.3.1 FPT\_STM\_EXT.1 TSS 1 [TD0632]

Objective	<p>If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.</p>
Evaluator Findings	<p>The evaluator examined the <b>FPT_STM_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE provides a source of date and time information used in audit event timestamps, and for certificate validity checking. The clock function is reliant on the system clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used in various routing protocols such as, OSPF, BGP, and ERF; Set system time, Calculate IKE stats (including limiting SAs based on times); determining AAA timeout, administrative session timeout, and SSH rekey.</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 5.9.3.2 FPT\_STM\_EXT.1 Guidance 1

Objective	<p>The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.</p> <p>If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>Clock Management</b> in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Clock management is restricted to the privileged administrator. Use the commands below to configuring the time and date:</b></p> <pre>router(config)# clock timezone zone hours-offset [minutes-offset] router(config)# clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]] router(config)# clock summer-time zone date date month year hh:mm:ss date month year hh:mm:ss [offset] router(config)# exit router# clock set hh:mm:ss date month year</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.9.4 FPT\_TST\_EXT.1.1

##### 5.9.4.1 FPT\_TST\_EXT.1.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.</p>
Evaluator Findings	<p>The evaluator examined the <b>FPT_TST_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS states that:</p> <ul style="list-style-type: none"> <li>• <b>AES Known Answer Test</b></li> </ul>

	<ul style="list-style-type: none"> <li>• <b>RSA Signature Known Answer Test (both signature/verification)</b></li> <li>• <b>RNG/DRBG Known Answer Test</b></li> <li>• <b>HMAC Known Answer Test</b></li> <li>• <b>SHA-1/256/384/512 Known Answer Test</b></li> <li>• <b>ECDSA self-test (both signature/verification)</b></li> <li>• <b>Software Integrity Test</b></li> </ul> <p>Additionally, the evaluator found that the descriptions of the test provide details of what the tests are actually doing (rather than a broad generalization of the test).</p> <p>The evaluator examined the <b>FPT_TST_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.4.2 FPT\_TST\_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled <b>Modes of Operation</b> in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>If any of the POST fails, the following actions should be taken:</b></p> <ul style="list-style-type: none"> <li>• <b>If possible, review the crashinfo file. This will provide additional information on the cause of the crash.</b></li> <li>• <b>Restart the TOE to perform POST and determine if normal operation can be resumed.</b></li> <li>• <b>If the problem persists, contact Cisco Technical Assistance via <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> or 1 800 553-2447.</b></li> <li>• <b>If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.</b></li> </ul> <p>If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated.</p> <p><b>Example Error Message:</b></p> <p><b>*Nov 26 16:28:23.629: %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failedFIPS-2-</b></p> <p><b>If a software upgrade fails, the router will display an error when an authorized administrator tries to boot the system. The router will then boot into the rommon prompt.</b></p> <p><b>Directory an_image.bin not found</b></p>

	<p><b>Unable to locate an_image.bin directory</b></p> <p><b>Unable to load an_image.bin</b></p> <p><b>boot: error executing "boot harddisk:an_image.bin"</b></p> <p><b>autoboot: boot failed, restarting</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.5 FPT\_TST\_EXT.3

5.9.5.1 FPT\_TST\_EXT.3 TSS

Objective	The evaluator verifies that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR.
Evaluator Findings	<p>The evaluator examined the <b>FPT_TST_EXT.3</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The integrity of stored TSF executable code when it is loaded for execution can be verified through the use of RSA and Elliptic Curve Digital Signature algorithms.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.6 FPT\_TUD\_EXT.1

5.9.6.1 FPT\_TUD\_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	<p>The evaluator examined the <b>FPT_TUD_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An Authorized Administrator can query the software version running on the TOE and can initiate updates to software images. The current active version can be verified by executing the "show version" command from the TOE's CLI. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.cisco.com.</b></p> <p>The TOE does not support delayed activation. The uploading of the TOE firmware and selection of the boot image are a manual process.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.9.6.2 FPT\_TUD\_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	<p>The evaluator examined the <b>FPT_TUD_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>To verify the digital signature prior to installation, the “show software authenticity file” command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. If the output from the “show software authenticity file” command does not provide the expected output, contact Cisco Technical Assistance Center (TAC)</b>  <a href="https://tools.cisco.com/ServiceRequestTool/create/launch.do">https://tools.cisco.com/ServiceRequestTool/create/launch.do</a>.</p> <p>The evaluator examined the <b>FPT_TUD_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.6.3 FPT\_TUD\_EXT.1 TSS 3

Objective	If the options ‘support automatic checking for updates’ or ‘support automatic updates’ are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains
-----------	---

	what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	The evaluator examined the Security Target and found that the options ‘support automatic checking for updates’ or ‘support automatic updates’ are not chosen from the selection in FPT_TUD_EXT.1.2  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.6.4 FPT\_TUD\_EXT.1 TSS 5

Objective	If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.
Evaluator Findings	The evaluator examined the <b>FPT_TUD_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that:  <b>Digital signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded.</b>  <b>The cryptographic hashes (i.e., SHA-512) are used to verify software update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. Authorized Administrators can download the approved image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. The verification should not be performed on the TOE during the update process. If the hashes do not match, contact Cisco Technical Assistance Center (TAC).</b>  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.6.5 FPT\_TUD\_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed
-----------	--



	activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	<p>The evaluator examined the section titled <b>Secure Acceptance of the TOE</b> in the AGD to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Step 11 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the “show version” command [8] to display the currently running system image filename and the system software release version. It is also recommended the license level be verified and activated as described in [13]. It is assumed the end-user has acquired a permanent license is valid for the lifetime of the system on which it is installed.</b></p> <p>The TOE does not support delayed activation. The uploading of the TOE firmware and selection of the boot image are a manual process.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.6.6 FPT\_TUD\_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled <b>Secure Acceptance of the TOE</b> in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that :</p> <p><b>Step 8 Once the file is downloaded, verify that it was not tampered with by using a SHA-512 utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 5 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), <a href="https://www.cisco.com/c/en/us/support/index.html">https://www.cisco.com/c/en/us/support/index.html</a>.</b></p> <p><b>Step 9 To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file.</b></p> <p><b>If the output from the show software authenticity file command does not provide expected output as described in [1], contact Cisco Technical Assistance Center (TAC) <a href="https://tools.cisco.com/ServiceRequestTool/create/launch.do">https://tools.cisco.com/ServiceRequestTool/create/launch.do</a>.</b></p> <p><b>After verifying the digital signature with the show software authenticity file command, an upgrade and reboot should be configured on the router as described in [1]. The router will not boot if the digital signature is not valid, and an error will be displayed on the console:</b></p>

	<p><b>autoboot: boot failed, restarting...</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.9.6.7 FPT\_TUD\_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	<p>The evaluator examined the section titled <b>Secure Acceptance of the TOE</b> in the AGD to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Step 8 Once the file is downloaded, verify that it was not tampered with by using a SHA-512 utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 5 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), <a href="https://www.cisco.com/c/en/us/support/index.html">https://www.cisco.com/c/en/us/support/index.html</a>.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.9.6.8 FPT\_TUD\_EXT.1 Guidance 6

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.
Evaluator Findings	<p>The evaluator examined the Security Target and verified that a certificate-based mechanism is not used for software update digital signature verification.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 5.10 TSS and Guidance Activities (TOE Access)

#### 5.10.1 FTA\_SSL\_EXT.1

##### 5.10.1.1 FTA\_SSL\_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking, or termination is supported and the related inactivity time period settings.
Evaluator Findings	The evaluator examined the <b>FTA_SSL_EXT.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies whether local

	<p>administrative session locking, or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “session-timeout” setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session.</b></p> <p><b>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.1.2 FTA\_SSL\_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	<p>The evaluator examined the section titled <b>Session Termination</b> in the AGD to verify that it states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting</b></p> <pre> TOE-common-criteria(config)# line vty &lt;first&gt; &lt;last&gt; TOE-common-criteria(config-line)# exec- timeout &lt;time&gt; TOE-common-criteria(config- line)# line console  TOE-common-criteria(config)# exec-timeout &lt;time&gt; </pre> <p><b>where first and last are the range of vty lines on the box (i.e. “0 15”), and time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the privileged administrator (see Section 4.1).</b></p> <p><b>The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	<p>The evaluator examined the <b>FTA_SSL_EXT.3</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “session-timeout” setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session</b></p> <p><b>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.
Evaluator Findings	<p>The evaluator examined the section titled <b>Session Termination</b> in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting</b></p> <p style="padding-left: 40px;"><b>TOE-common-criteria(config)# line vty &lt;first&gt;</b>  <b>&lt;last&gt; TOE-common-criteria(config-line)# exec-</b>  <b>timeout &lt;time&gt; TOE-common-criteria(config-</b>  <b>line)# line console</b></p> <p style="padding-left: 40px;"><b>TOE-common-criteria(config)# exec-timeout &lt;time&gt;</b></p> <p><b>where first and last are the range of vty lines on the box (i.e. “0 15”), and time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the privileged administrator (see Section 4.1).</b></p> <p><b>The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.</b></p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3 FTA\_SSL.4

5.10.3.1 FTA\_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	<p>The evaluator examined the <b>FTA_SSL_EXT.4</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” or “logout” command.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.3.2 FTA\_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	<p>The evaluator examined the section titled <b>Remote Administration Protocols</b> in the AGD to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>To terminate a remote or local session to the router, use the “exit” or “logout” command at the User or Privilege EXEC prompt to terminate the session.</b></p> <p><b>Router# exit</b> <b>or</b> <b>Router# logout</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.4 FTA\_TAB.1

5.10.4.1 FTA\_TAB.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for
-----------	--

	different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).
Evaluator Findings	<p>The evaluator examined the <b>FTA_TAB.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.10.4.2 FTA\_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	<p>The evaluator examined the section titled <b>Login Banners</b> in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>The TOE may be configured by the privileged administrators with banners using the banner login command. This banner is displayed before the username and password prompts. To create a banner of text “This is a banner” use the command</b></p> <p><b>banner login d This is a banner d</b></p> <p><b>where d is the delimiting character. The delimiting character may be any character except ‘?’, and it must not be part of the banner message.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 5.11 TSS and Guidance Activities (Trusted Path/Channels)

#### 5.11.1 FTP\_ITC.1

##### 5.11.1.1 FTP\_ITC.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the <b>FTP_ITC.1</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the

	<p>method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The TOE requires that peers and other TOE instances establish an IKE/IPSec connection in order to forward routing tables used by the TOE.</b></p> <p><b>The TOE protects communications between the TOE and the remote audit server using IPsec. This provides a secure channel to transmit the log events. Likewise communications between the TOE and AAA servers are secured using IPsec.</b></p> <p><b>The distinction between “remote VPN gateway” and “another instance of the TOE” is that “another instance of the TOE” would be installed in the evaluated configuration, and likely administered by the same personnel, whereas a “remote VPN gateway/peer” could be any interoperable IPsec gateway/peer that is expected to be administered by personnel who are not administrators of the TOE, and who share necessary IPsec tunnel configuration and authentication credentials with the TOE administrators. For example, the exchange of X.509 certificates for certificate based authentication.</b></p> <p><b>MACsec is also used to secure communication channels between MACsec peers at Layer 2.</b></p> <p><b>The TOE acts as a server for both IPsec and MACsec secure channels.</b></p> <p>The evaluator examined the <b>FCS_COP.1/DataEncryption</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that</p> <p><b>The TOE provides AES encryption and decryption in support of IPsec and SSHv2 for secure communications.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.1.2 FTP\_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	<p>The evaluator examined the <b>IPsec Overview, Logging Protection, Authentication Server Protocols, MACsec and MKA Configuration</b> in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD states that:</p> <p><b><u>IPsec Overview</u></b>  <b>This section provides details on establishing IPsec sessions with an authorized entity and recovery instructions.</b></p> <p><b><u>Logging Protection</u></b></p>

	<p>If an authorized administrator wants to backup the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:</p> <ol style="list-style-type: none"> <li>1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or</li> <li>2. With a syslog server not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network.</li> </ol> <p><b><u>Authentication Server Protocols</u></b></p> <p>RADIUS (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but should be enabled by administrators in the evaluated configuration.</p> <p>To configure RADIUS, refer to [5]. Use best practices for the selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.</p> <p>These protocols are to be tunneled over an IPsec connection in the evaluated configuration. The instructions for setting up this communication are the same as those for protecting communications with a syslog server, detailed in Section 3.3.5 below.</p> <p><b><u>MACsec and MKA Configuration</u></b></p> <p>This section provides an online reference containing appropriate instructions on configuring the MACsec trusted channel and recovery instructions.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.2 FTP\_ITC.1/VPN

5.11.2.1 FTP\_ITC.1/VPN TSS 1

Objective	<p>The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.</p> <p>From FTP_ITC.1:</p> <p>The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.</p>
Evaluator Findings	<p>The evaluator examined the <b>FTP_ITC.1/VPN</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism</p>



	<p>is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>The distinction between “remote VPN gateway” and “another instance of the TOE” is that “another instance of the TOE” would be installed in the evaluated configuration, and likely administered by the same personnel, whereas a “remote VPN gateway/peer” could be any interoperable IPsec gateway/peer that is expected to be administered by personnel who are not administrators of the TOE, and who share necessary IPsec tunnel configuration and authentication credentials with the TOE administrators. For example, the exchange of X.509 certificates for certificate based authentication.</b></p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.11.2.2 FTP\_ITC.1/VPN Guidance

Objective	<p>The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.</p> <p>From FTP_ITC.1:</p> <p>The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.</p>
Evaluator Findings	<p>The evaluator examined the section titled <b>Virtual Private Networks</b> in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD states that:</p> <p><b>IPsec provides secure <i>tunnels</i> between two peers, such as two routers. The privileged administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.</b></p> <p>The evaluator found that the only allowed protocols is IPsec and it’s configuration is given in section titled <b>IPsec Overview</b>.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.11.3 FTP\_TRP.1/Admin

##### 5.11.3.1 FTP\_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The
-----------	--

	evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.
Evaluator Findings	<p>The evaluator examined the <b>FTP_TRP.1/Admin</b> entry in section titled <b>TOE Summary Specification</b> in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that:</p> <p><b>All remote administrative communications take place over a secure encrypted SSHv2 session which has the ability to be encrypted further using IPsec. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.</b></p> <p>Next, the evaluator compared the protocols identified in the TSS to the definition of the SFR. The evaluator found that the protocols listed in the TSS are consistent with the protocols listed in the definition of the SFR.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

#### 5.11.3.2 FTP\_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	<p>The evaluator examined the sections titled <b>Remote Administration Protocols</b> and <b>IPsec Overview</b> in the AGD to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that both the AGDs provide instructions for configuring the remote administration of the TOE.</p> <p>In particular, the evaluator found that these instructions include configuration of the protocols used to secure remote administrative session. Specifically, the AGD provides instructions for configuring the following protocols: SSH and IKE/IPsec</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 6 Detailed Test Cases (Test Activities)

### 6.1 FAU\_GEN.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&amp;A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.</p> <p>Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Trigger each auditable event on the TOE</li> <li>• Verify that each audit record is generated and contains the appropriate audit record details</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to generate audit records for each of the events described in the ST under the FAU_GEN.1.1, FAU_GEN.1.2.</li> <li>• The audit records generated should match the proper format as specified in the guidance documentation.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The audit records associated with each test case are recorded with each test case. A comparison of required audit records to the presented audit records was additionally performed. This analysis shows that each required audit record is generated by the TOE, meeting the test requirements.</p>

### 6.1 FAU\_STG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that Passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the version of audit syslog server.</li> <li>• Configure the TOE for IPsec connection</li> <li>• Configure the VM for IPsec connection</li> <li>• Verify that the tunnel has been established</li> <li>• Verify in the Syslog Server that the logs are captured</li> <li>• Verify in the TOE logs that the logs are captured</li> <li>• Verify via packet capture that the IPsec traffic is not sent in clear text</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence showing that logs generated on the TOE are the same as those transferred to the external audit server.</li> <li>• Packet capture showing that logs sent to the external audit server are encrypted.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.

## 6.2 FAU\_STG\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that:</p> <p>The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '<b>overwrite previous audit records</b>' in FAU_STG_EXT.1.3)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Set the audit log to a new limit (4096 bytes)</li> <li>• Verify oldest log in storage</li> <li>• Generate some new audit logs</li> <li>• Check logs again. Old logs were overwritten with new logs</li> </ul>
<b>Expected Test Results</b>	The TOE should overwrite the previous audit records when the local audit space is filled.
<b>Pass/Fail with Explanation</b>	Pass. When audit data is filled to the max, the existing audit data is overwritten.

## 6.3 FPT\_STM\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: If the TOE supports direct <b>setting of the time by the Security Administrator</b> , then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm current time set on TOE</li> <li>• Remove NTP settings if any</li> <li>• Set time</li> <li>• Verify that the new time was set</li> <li>• Check logs</li> </ul>
<b>Expected Test Results</b>	TOE should support Time set by Security Admin and also reflect in Logs.
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows the administrative user to configure the time on the TOE. This meets the testing requirements.

## 6.4 FTP\_ITC.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
<b>Test Steps</b>	<p>Authentication Server:</p> <ul style="list-style-type: none"> <li>• Configure the TOE and VM for IPsec using strongswan from FAU_STG_EXT.1 Test #1</li> <li>• Configure RADIUS server on TOE</li> <li>• Configure RADIUS server on VM</li> <li>• Verify that the tunnel is up</li> <li>• Generate traffic by authenticating to the TOE</li> <li>• Verify via logs that the session was established</li> <li>• Verify the TOE can successfully communicate with the authentication server via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should initiate connection to a remote AAA server (Radius) over IPsec</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE can be configured to successfully communicate with the external audit server, remote authentication server and remote VPN peers via IPsec. The audit server test is covered in FAU_STG_EXT.1 Test #1

## 6.5 FTP\_ITC.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
<b>Pass/Fail with Explanation</b>	Pass. This test is performed in conjunction with the tests associated with FTP_ITC.1 Test# 1, FAU_STG_EXT.1 and FCS_IPSEC_EXT.1. The TOE initiates the session to the external entity. This meets the testing requirements

## 6.6 FTP\_ITC.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
<b>Pass/Fail with Explanation</b>	Pass. This test is performed in conjunction with the tests associated with FTP_ITC.1 Test# 1, FAU_STG_EXT.1 and FCS_IPSEC_EXT.1. External connections from the TOE are sent via an encrypted channel. This meets the testing requirements.

## 6.7 FTP\_ITC.1 Test #4

Item	Data
<b>Test Assurance Activity</b>	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.

	<p>The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations:</p> <ol style="list-style-type: none"> <li>i. A duration that exceeds the TOE’s application layer timeout setting,</li> <li>ii. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer.</li> </ol> <p>The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.</p> <p>In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure an IPsec tunnel from TOE to Peer.</li> <li>• Interrupt the connection between the devices for a duration shorter than the application layer timeout but of sufficient length to interrupt the MAC layer and verify that connection is down.</li> <li>• Verify that the traffic is encrypted when connection was restored.</li> <li>• TOE Logs.</li> <li>• Interrupt the connection between the devices for a duration that exceeds the TOE’s application layer timeout setting and verify that connection is down.</li> <li>• Verify that the traffic is encrypted when connection was restored.</li> <li>• TOE Logs.</li> </ul> <p>Note: The same steps were performed with MACsec on each device for an immediate duration and for at least 2 seconds. Physically disrupting the cabling would result in the bridge used to capture packets being interrupted and thus it was not possible to capture the entire session (packet captures would only show MACsec frames before and after the disconnect). In all cases the MACsec connection was active upon bringing the bridge back up. Evidence of successful MACsec frames is shown throughout FCS_MACSEC_EXT.1 testing</p>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Traffic between remote end point and itself should be secure after several interruptions.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TOE does not send plaintext traffic when disconnected from the external entity. This meets the testing requirements.</p>

## 6.8 FCS\_CKM.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p><b>FFC Schemes using “safe-prime” groups</b></p> <p>The evaluator shall verify the correctness of the TSF’s implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.</p> <p><b>TD0580 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	<p>Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test #1 and FTP_ITC.1 Test 1 to demonstrate correct operation.</p>

## 6.9 FIA\_AFL.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any Passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to lock out a user after three failed login attempts.</li> <li>• Log in to the TOE with invalid credentials until user is locked out.</li> <li>• Verify that user is locked.</li> <li>• Verify with logs that attempts with invalid credentials are rejected.</li> <li>• Attempt to log in with the locked account and good credentials.</li> <li>• Verify with logs that the TOE rejects the login attempt.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should not allow authentication once the authentication attempt limit has been reached.</li> <li>• Evidence (screenshot or CLI output) showing configuration of maximum authentication attempts.</li> <li>• Log showing user getting locked out since the maximum limit is reached.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TOE did not allow authentication once the authentication attempt limit has been reached. This meets the testing requirements.</p>

## 6.10 FIA\_AFL.1 Test #2a

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any Passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:</p> <p>If the <b>administrator action</b> selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the user is locked</li> <li>• Manually unlock the user account</li> <li>• Login with good credentials</li> <li>• Verify that the lockout has been removed</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should not allow authentication until the locked-out user was manually unlocked</li> <li>• Evidence (screenshot or CLI output) showing manual unlock of locked-out user</li> <li>• Log showing successful session establishment after unlocking</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. The TOE allowed authentication after the locked-out user was manually unlocked. This meets the testing requirements.
-----------------------------------	--

### 6.11 FIA\_PMG\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall compose Passwords that meet the requirements in some way. For each Password, the evaluator shall verify that the TOE supports the Password. While the evaluator is not required (nor is it feasible) to test all possible compositions of Passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing. <b>TD0571 has been applied</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configuring the Password requirements.</li> <li>• Attempt to create good Password that is “QWEyuiop()12345”. (15-character Password, the combination of 3 upper, 5 lower, 5 numeric and 2 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create a good Password that is “ASDGHjklz@#%789”. (15-character Password, the combination of 5 upper, 4 lower, 3 numeric and 3 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create good Password that is “LZXblk&amp;^%\$#9359”. (15-character Password, the combination of 3 upper, 3 lower, 4 numeric and 5 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create a good Password that is “HJTpoi\$!*\$!&amp;670”. (15-character Password, the combination of 3 upper, 3 lower, 3 numeric and 6 special characters)</li> <li>• Show that the new user is created.</li> <li>• Attempt to create good Password that is “VBNMfghj)&amp;%5437”. (15-character Password, combination of 4 upper, 4 lower, 4 numeric and 3 special characters)</li> <li>• Show that the new user is created.</li> <li>• Show log.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should allow the creation of users whose Passwords meet the requirements.</li> <li>• Evidence (screenshot or CLI output) of each Password creation attempt.</li> <li>• Logs showing the successful Password creation.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE was able to create users with good Passwords. This meets the requirement.

### 6.12 FIA\_PMG\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall compose Passwords that do not meet the requirements in some way. For each Password, the evaluator shall verify that the TOE does not support the Password. While the evaluator is not required (nor is it feasible) to test all possible compositions of Passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing. <b>TD0571 has been applied</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to create a bad Password that is “QWEyuiop()123”.</li> </ul>



	<p>(combination of 2 upper, 6 lower, 3 numeric &amp; 2 special characters)</p> <ul style="list-style-type: none"> <li>Attempt to create a bad Password "ASDGHJKI" (combination of 7 upper,1 lower characters)</li> <li>Attempt to create bad Password "k&amp;^%\$#93". (1 lower, 2 numeric characters &amp; 5 special characters)</li> <li>Attempt to create bad Password "k67098". (1 lower &amp; 5 numeric characters)</li> <li>Verify that the user is not created.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should reject Passwords that do not meet the specified requirements.</li> <li>Evidence (screenshot or CLI output) of each Password creation attempt.</li> <li>showing the unsuccessful Password creation.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE was able to reject users with bad Passwords. This meets the requirement.

### 6.13 FIA\_UIA\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:</p> <p>Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&amp;A information results in the ability to access the system, while providing incorrect information results in denial of access.</p>
<b>Test Steps</b>	<p>CONSOLE</p> <ul style="list-style-type: none"> <li>Log onto the TOE local connection with incorrect credentials.</li> <li>Log onto the TOE local connection with correct credentials.</li> <li>Verify the logs reflect for incorrect credentials.</li> <li>Verify the logs reflect for correct credentials.</li> </ul> <p>SSH</p> <ul style="list-style-type: none"> <li>Log onto the TOE remote SSH CLI connection with incorrect credentials.</li> <li>Log onto the TOE remote SSH CLI with correct credentials.</li> <li>Verify the logs reflect for incorrect credentials.</li> <li>Verify the logs reflect for correct credentials.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should deny access when incorrect authentication credentials are presented and allow access when correct authentication credentials are presented.</li> <li>Evidence (screenshot or CLI output) of each authentication attempt.</li> <li>Logs showing successful/unsuccessful authentication attempts.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements

### 6.14 FIA\_UIA\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Connect to the TOE remotely using ssh and verify the only option presented is the username/Password entry and give incorrect credentials. It is seen that only the login banner is displayed prior to authentication.</li> <li>• Verify authentication logs reflect failure.</li> <li>• Attempt to connect to the TOE with correct credentials remotely and verify that the previously disabled commands are now available.</li> <li>• Verify authentication logs reflect success.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• No services except displaying a banner is available to a remote administrator attempting to login to the TOE via SSH.</li> <li>• Log showing inability to access any services prior to login.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. No system services are available to an unauthenticated user connecting remotely. It is seen that only the login banner is displayed prior to authentication. This meets the testing requirements.

### 6.15 FIA\_UIA\_EXT.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Connect to the TOE via console and verify the only option presented is the username/Password entry. It is seen that only the login banner is displayed prior to authentication.</li> <li>• Verify the logs reflected. Following audit logs are generated on TOE and they are manually copied from the console and pasted in this test plan.</li> <li>• Attempt to connect to the TOE with correct credentials.</li> <li>• Verify authentication logs reflect success.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• No services except displaying a banner is available to a local administrator attempting to login to the TOE.</li> <li>• Log showing inability to access any services prior to login.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. No system services are available to an unauthenticated user via the directly connected console. It is seen that only the login banner is displayed prior to authentication. This meets the testing requirements.

### 6.16 FIA\_UAU.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Connect to the TOE via console with correct authentication credentials and verify that at most obscured feedback is provided.</li> <li>• Verify authentication logs reflect success</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should not provide anything other than obscured feedback at the directly connected login prompt.</li> <li>• Evidence (screenshot or CLI output) showing no output from the Password being entered.</li> <li>• Logs show successful/unsuccessful login attempts.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE obscures Password. This meets testing requirements.

### 6.17 FMT\_MOF.1/ManualUpdate Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login to the TOE via a lower privileged user.</li> <li>• Attempt to access configuration mode without the proper privilege and verify user is unable to access it.</li> <li>• Attempt to perform an update command and verify the command is rejected.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject attempts from an unprivileged user to update a legitimate image on the TOE</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Unprivileged user cannot perform a software update on the TOE. This meets the testing requirements.

### 6.18 FMT\_MOF.1/ManualUpdate Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log into the TOE as a privileged user.</li> <li>• Verify user can access configuration mode.</li> <li>• Copy the update image to the flash.</li> <li>• Attempt an update command and verify it succeeds.</li> <li>• Verify via logs.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should accept attempts from a privileged user to update a legitimate image on the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. A privileged user is able to perform a software update on the TOE. This meets the testing requirements

### 6.19 FMT\_MOF.1/Functions (1) Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1 (if ' <b>transmission of audit data to external IT entity</b> ' is selected from the second selection together with ' <b>modify the behaviour of</b> ' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Connect to the TOE as unprivileged user.</li> <li>Attempt to modify the parameters involved with the syslog server and verify the command is rejected.</li> <li>Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should reject attempts from an unprivileged user to modify audit data on the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not allow an unauthenticated user to modify and delete the audit records.

### 6.20 FMT\_MOF.1/Functions (1)Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2 (if ' <b>transmission of audit data to external IT entity</b> ' is selected from the second selection together with ' <b>modify the behaviour of</b> ' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
<b>Pass/Fail with Explanation</b>	Pass. This testing is covered by the requirements in FAU_STG_EXT.1.

### 6.21 FMT\_MOF.1/Services Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable this service/these services can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log into the TOE as a lower privileged user.</li> <li>• Attempt to modify the parameters; This will fail.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should not allow attempts to enable and disable the services without prior authentication as security administrator.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. User without prior authentication/privilege was unable to perform actions on the TOE.

### 6.22 FMT\_MOF.1/Services Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Login to the TOE as an admin.</li> <li>• Attempt to modify service parameters and verify the command is accepted.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should allow attempts to enable and disable the services with prior authentication as security administrator.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. User with prior authentication/privilege was able to perform actions on the TOE.

### 6.23 FMT\_MTD.1/CryptoKeys Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access

	control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Connect to the TOE as unprivileged user.</li> <li>• Attempt to enter conf mode and verify it is rejected.</li> <li>• Attempt to perform a configuration command to modify crypto key and verify the command is rejected.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject attempts from an unprivileged user to modify, delete, generate/import crypto keys on the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Unprivileged user cannot perform security related configurations on the TOE. This meets the testing requirements.

#### 6.24 FMT\_MTD.1/CryptoKeys Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Authenticate to the TOE as an admin</li> <li>• Enter enable mode/config mode</li> <li>• Attempt to set a configuration command to modify the crypto key. Verify it succeeds</li> <li>• Verify the audit via log</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should accept attempts from a privileged user to modify, delete, generate/import crypto keys on the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Authenticated user can perform security related configurations on the TOE. This meets the testing requirements.

#### 6.25 FMT\_SMF.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
<b>Expected Test Results</b>	All management functions identified in Security Target should be met by presenting correct test cases.
<b>Pass/Fail with Explanation</b>	Pass. Throughout the various security functionality testing of the TOE, FMT_SMF.1 Specification of Management Functions requirements have been met. Therefore, this test is Passed.

### 6.26 FMT\_SMR.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
<b>Pass/Fail with Explanation</b>	Pass. There are 2 different interfaces where these can be tested (console/Remote CLI) and all test cases use these interfaces. The evaluator has met this requirement through the execution of the entirety of this test report by performing actions via all 2 interfaces.

### 6.27 FTA\_SSL.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log into the TOE via SSH.</li> <li>• Configure new idle time (60 seconds).</li> <li>• Verify that a log was created for the configuring the timeout period.</li> <li>• Log into the TOE via SSH.</li> <li>• Wait 60 seconds and attempt a command.</li> <li>• Verify that a log was created for inactivity logout.</li> <li>• Configure new idle time (120 seconds).</li> <li>• Verify that a log was created for the configuring the timeout period.</li> <li>• Log into the TOE via SSH.</li> <li>• Wait 120 seconds and attempt a command.</li> <li>• Verify that a log was created for inactivity logout</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should terminate idle remote sessions after the configured time.</li> <li>• Evidence (e.g., screenshot or CLI output) showing configuration of time out value.</li> <li>• Log showing the administrative log on (with time).</li> <li>• Evidence (e.g., screenshot or CLI output) showing administrator being terminated.</li> <li>• Log showing the termination of the connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	The remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements.

### 6.28 FTA\_SSL.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log onto the TOE through local administrative interface.</li> <li>• Verify the logs reflect the log in.</li> <li>• Using the instructions provided by the user guide log off.</li> <li>• Verify the logs reflect the log off.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should allow the user to terminate the directly connected administrative sessions.</li> <li>• Log showing the log out.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.

## 6.29 FTA\_SSL.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log onto the TOE through ssh administrative interface.</li> <li>• Verify the logs reflect log in.</li> <li>• Using the instructions provided by the user guide log off.</li> <li>• Verify the logs reflect log in</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should allow the user to terminate the interactive remote sessions.</li> <li>• Log showing the log out</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.

## 6.30 FTA\_SSL\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Log into the TOE via Console.</li> <li>• Configure new idle time (60 seconds).</li> <li>• Verify that a log was created for the configuring the timeout period.</li> <li>• Log into the TOE via Console and wait 60 seconds and attempt a command.</li> <li>• Verify that a log was created for inactivity logout.</li> <li>• Configure new idle time (120 seconds).</li> <li>• Verify that a log was created for the configuring the timeout period.</li> <li>• Log into the TOE via Console and wait 120 seconds and attempt a command.</li> <li>• Verify that a log was created for inactivity logout.</li> </ul>



<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should terminate idle local sessions after the configured time.</li> <li>• Evidence (e.g., screenshot or CLI output) showing configuration of time out value.</li> <li>• Log showing the administrative log on (with time).</li> <li>• Evidence (e.g., screenshot or CLI output) showing administrator being terminated.</li> <li>• Log showing the termination of the connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.

### 6.31 FTA\_TAB.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure access banners on TOE.</li> <li>• Log into the TOE via SSH.</li> <li>• Verify that the audit records reflected the configuration steps.</li> <li>• Configure access banners on TOE.</li> <li>• Log into the TOE via console.</li> <li>• Verify that the audit records reflected.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• When any user accesses the TOE through the console and SSH, the configured banner should be displayed prior to authenticating the TOE.</li> <li>• Evidence (e.g., screenshot or CLI output) showing configuration of access banners.</li> <li>• Log showing configuration of the access banners.</li> <li>• Evidence (e.g., screenshot or CLI output) from logon with access banners.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.

### 6.32 FTP\_TRP.1/Admin Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to establish an SSH connection from a remote administrator.</li> <li>• Capture the traffic between the devices and verify that traffic was not sent in plaintext.</li> <li>• Verify that the session was established via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should establish communication between TOE and remote administrator via SSH and IPsec.</li> <li>• The ESP packets in IPsec connection and Encrypted Packets in SSH connection in packet capture should confirm that the data is not sent in plain text.</li> <li>• Evidence (screenshot or CLI output) showing attempt to connect via the trusted paths</li> <li>• Log showing successful connection</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. Remote administrative access to the TOE is over secure protected channels and the data was not sent in plaintext. IPSEC is covered by FCS_IPSEC_EXT.1. This meets the testing requirements.
-----------------------------------	---

### 6.33 FTP\_TRP.1/Admin Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
<b>Pass/Fail with Explanation</b>	Pass. This test is covered by FTP_TRP.1/Admin_T1, FCS_SSH_EXT.1 and FCS_IPSEC_EXT.1. In that test, the data was not sent in plaintext.

### 6.34 FCS\_SSHS\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test objective: The purpose of these tests is to verify server supports each claimed client authentication method.</p> <p>Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. <b>TD0631 has been applied</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Generate the ssh-rsa pub key.</li> <li>• Configure the TOE to support RSA based SSH authentication method.</li> <li>• Log into the TOE SSH with RSA-based authentication.</li> <li>• Verify authentication via packet capture.</li> <li>• Verify authentication via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support successful negotiations when using the claimed public key algorithm (ssh-rsa) and reject SSH connections when using a non-approved algorithm.</li> <li>• Log showing successful/unsuccessful connection of each algorithm.</li> <li>• Packet capture showing successful/unsuccessful connection of each algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed public key algorithm. This meets the testing requirements.

### 6.35 FCS\_SSHS\_EXT.1.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. <b>TD0631 has been applied</b>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the SSH client with a new RSA keypair for SSH without configuring the TOE and attempt to login using ssh-rsa key.</li> <li>• Log into the TOE SSH using RSA-based authentication.</li> <li>• Verify authentication failure via packet capture.</li> <li>• Verify authentication logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject SSH connections when incorrect/unknown public keys are presented.</li> <li>• Evidence (screenshot or CLI output) of attempting to authenticate the TOE.</li> <li>• Packet capture of unsuccessful authentication.</li> <li>• Log showing unsuccessful authentication.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not allow public key authentication if the public key of the SSH user have not uploaded to the TOE. This meets the test requirements.

### 6.36 FCS\_SSHS\_EXT.1.2 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3: [Conditional] If Password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept Password-based authentication and demonstrate that user authentication succeeds when the correct Password is provided by the connecting SSH client. <b>TD0631 has been applied</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Ensure the TOE supports Password-based authentication.</li> <li>• Log into the TOE via SSH with Password authentication.</li> <li>• Verify authentication logs.</li> <li>• Verify via packet capture that SSH session was established.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should set up a user with Password-based authentication.</li> <li>• User authentication succeeds when the correct Password is provided by the user.</li> <li>• Packet capture of session being established.</li> <li>• Log showing successful authentication.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to accept Password authentication from a remote SSH client. This meets the testing requirements.

### 6.37 FCS\_SSHS\_EXT.1.2 Test #4

Item	Data
<b>Test Assurance Activity</b>	Test 4: [Conditional] If Password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept Password-based authentication and demonstrate that user authentication fails when the incorrect Password is provided by the connecting SSH client. <b>TD0631 has been applied</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Ensure the TOE supports Password-based authentication.</li> <li>• Attempt to Log into the TOE via SSH with correct username incorrect Password-based authentication parameters (will fail).</li> <li>• Verify authentication via logs that reflect failures.</li> <li>• Verify authentication via packet captures that reflect failures.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should set up a user with Password-based authentication.</li> <li>• User authentication fails when the incorrect Password is provided by the user.</li> <li>• Packet capture of failed connection.</li> </ul>

	<ul style="list-style-type: none"> <li>• Log showing unsuccessful authentication</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements.

### 6.38 FCS\_SSHS\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use acumen-sshs tool to send packets greater than 65,535 bytes to TOE</li> <li>• Verify authentication logs reflect failures</li> <li>• Verify the TOE rejects the connection attempt via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should drop packets larger than the allowed range.</li> <li>• Log showing the reason for closing the connection.</li> <li>• Packet capture showing TOE closes the connection when packet sent is larger than allowed range.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements.

### 6.39 FCS\_SSHS\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.</p> <p>To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test.</p> <p>If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for SSH</li> <li>• Connect to the TOE using aes128-cbc</li> <li>• Verify that the SSH session was encrypted using aes128-cbc via capture</li> <li>• Verify that the SSH session was encrypted using aes128-cbc via log</li>   <li>• Establish an SSH session with the configured supported algorithms (aes256-cbc)</li> <li>• Verify that the SSH session was encrypted using aes256-cbc via capture</li> <li>• Verify that the SSH session was encrypted using aes256-cbc via log</li>   <li>• Establish an SSH session with the unclaimed algorithms.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify the failure via audit log.</li> <li>• Verify the failure via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support successful negotiations when using the claimed ciphersuites (AES-128 &amp; AES-256) and reject SSH connections. when using a non-approved algorithm.</li> <li>• Log showing successful/unsuccessful connection of each algorithm.</li> <li>• Packet capture showing successful/unsuccessful connection of each algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed algorithm and The TOE rejects SSH connections using a non-approved algorithm. This meets the testing requirements.

#### 6.40 FCS\_SSHS\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types. <b>TD0631 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the Claimed Host key algorithms by TOE. Screenshot of the TOE with Claimed Host key algorithms by TOE</li> <li>• Established a session with the TOE using the rsa-sha2-256 host key algorithms.</li> <li>• Verify through logs</li> <li>• Verify through packet capture that the SSH session was encrypted using host key algorithms.</li> <li>• Established a session with the TOE using the rsa-sha2-512 host key algorithms</li> <li>• Verify through logs</li> <li>• Verify through packet capture that the SSH session was encrypted using host key algorithms.</li> <li>• Established a session with the TOE using the ssh-rsa host key algorithms.</li> <li>• Verify through logs.</li> <li>• Verify through packet capture that the SSH session was encrypted using host key algorithms.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE allows client to connect using the supported Host public key algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows client to connect using the supported Host public key algorithm. This meets the testing requirements.

#### 6.41 FCS\_SSHS\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected.</p>

	Test objective: This negative test case is meant to validate that the TOE server does not support host public key algorithms that are not claimed. <b>TD0631 has been applied.</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the Claimed Host key algorithms by TOE</li> <li>• Established a session with the TOE using the non-supported host key algorithms (SSH-DSS)</li> <li>• Verify through logs that the SSH session was not established.</li> <li>• Verify through packet capture that the SSH session was not established.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• TOE should reject the connection if the session is established using a non-supported host key algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE rejects the connection if the session is established using a non-supported host key algorithm. This meets the testing requirement.

#### 6.42 FCS\_SSHS\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: [conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Establish an SSH session with the configured supported algorithms (HMAC-SHA2-256).</li> <li>• Verify that the SSH session was encrypted using HMAC-SHA2-256 via capture.</li> <li>• Verify that the message integrity algorithm used was as configured via log.</li> <li>• Establish an SSH session with the configured supported algorithms (HMAC-SHA2-512).</li> <li>• Verify that the SSH session was encrypted using HMAC-SHA2-512 via capture.</li> <li>• Verify that the message integrity algorithm used was as configured via log.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support successful negotiations when using the claimed message integrity algorithms (HMAC-SHA2-256, HMAC-SHA2-512) and reject SSH connections when using a non-approved algorithm.</li> <li>• Log showing successful/unsuccessful connection of each algorithm.</li> <li>• Packet capture showing successful/unsuccessful connection of each algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed data integrity algorithm. This meets the testing requirements.

#### 6.43 FCS\_SSHS\_EXT.1.6 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2: [conditional, if an <b>HMAC or AEAD_AES*_GCM</b> algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.</p>

	Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to establish an SSH session using HMAC-MD5-96</li> <li>• Verify via Wireshark that the TOE rejects the connection</li> <li>• Verify via logs</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE shall reject connection attempt for HMAC-MD5-96 integrity algorithm</li> <li>• Log showing successful/unsuccessful connection of algorithm.</li> <li>• Packet capture showing successful/unsuccessful connection of algorithm</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to make SSH connections with each claimed data integrity algorithm and The TOE rejects SSH connections using a non-approved algorithm. This meets the testing requirements

#### 6.44 FCS\_SSHS\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Attempt to establish an SSH session using diffiehellman-group1-sha1.</li> <li>• Verify that the TOE rejects the connection attempt via logs</li> <li>• Verify that the TOE rejects the connection via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support successful negotiations &amp; reject connections when using a non-approved method.</li> <li>• Log showing successful/unsuccessful connection of each method.</li> <li>• Packet capture showing successful/unsuccessful connection of each method.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements

#### 6.45 FCS\_SSHS\_EXT.1.7 Test #2

Item	Data
<b>Test Assurance Activity</b>	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Establish an SSH session with the configured supported diffie-hellman-group14-sha1.</li> <li>• Verify that the TOE rejects the connection attempt via logs.</li> <li>• Verify that the TOE rejects the connection attempt via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support successful negotiations when using the claimed key exchange method (diffiehellman-group14-sha1)</li> <li>• Log showing successful/unsuccessful connection of each method.</li> <li>• Packet capture showing successful/unsuccessful connection of each method.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE can use the claimed algorithm "diffie-hellman-group14-sha1" for SSH connection. This meets the testing requirements.

#### 6.46 FCS\_SSHS\_EXT.1.8 Test #1a

Item	Data
------	------



<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the <b>time-based threshold</b> and the traffic-based threshold.</p> <p>For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for SSH rekey with the time 10 minutes.</li> <li>• Establish an SSH session with the TOE and keep it idle for 10 MINs</li> <li>• Verify the TOE initiates a rekey for session keys</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should issue a rekey after the specified time is configured on the TOE.</li> <li>• Log showing session rekey request being sent after time-based threshold has been reached.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. TOE successfully rekeyed when the time limit was reached. This meets the testing requirements.</p>

#### 6.47 FCS\_SSHS\_EXT.1.8 Test #1b

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the <b>traffic-based</b> threshold.</p> <p>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8).</p> <p>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance</p>



	<p>documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p> <p>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:</p> <ol style="list-style-type: none"> <li>An argument is present in the TSS section describing this hardware- based limitation and</li> <li>All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Enabling time-out.</li> <li>Configuring the SSH REKEY with the volume 100000 KB.</li> <li>SSH Rekey Configuration Details.</li> <li>Establish an SSH session with the TOE and continually send traffic.</li> <li>Logging Details for Rekey based on volume.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should issue a rekey after the amount of data is transferred as configured on the TOE.</li> <li>Log showing session rekey request being sent after volume-based threshold has been reached.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE successfully rekeyed when the traffic limit was reached. This meets the testing requirements.

#### 6.48 FCS\_IPSEC\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPSEC implementation.
<b>Test Steps</b>	<p>PERMIT</p> <p><u>POSITIVE TEST</u></p> <ul style="list-style-type: none"> <li>Configure the TOE for with an SPD covering permit.</li> <li>Configure an IPsec connection to the TOE peer.</li> <li>Send traffic that is protected.</li> <li>Verify the established connection with IKE SA.</li> <li>Verify established connection with logs.</li> <li>Verify that each ACL was enforced via packet capture.</li> </ul> <p><u>NEGATIVE TEST</u></p> <ul style="list-style-type: none"> <li>Send traffic that does not match the configured ACL.</li> <li>Verify that there were no specific logs generated related to matching ACLs.</li> </ul>

	<ul style="list-style-type: none"> <li>Verify that the packet was unencrypted via packet capture.</li> </ul> <p>DENY</p> <p><u>POSITIVE TEST</u></p> <ul style="list-style-type: none"> <li>Configure the TOE for with an SPD covering deny.</li> <li>Configure the peer for with an SPD covering deny.</li> <li>Attempt to establish the connection.</li> <li>Verify the failed connection with logs.</li> <li>Verify that the packets were denied via the packet capture.</li> </ul> <p><u>NEGATIVE TEST</u></p> <ul style="list-style-type: none"> <li>Send traffic that does not match the configured ACL and hits the default rule.</li> <li>Verify that there were no specific logs generated related to matching ACLs.</li> <li>Verify that the packets were allowed via packet capture.</li> </ul> <p>BYPASS</p> <p><u>POSITIVE TEST</u></p> <ul style="list-style-type: none"> <li>Create an ACL to ByPass traffic from a host and then apply it to the respective crypto map/interface.</li> <li>Attempt to establish the connection.</li> <li>Verify the connection with logs.</li> <li>Verify that the packets were byPassed via Packet Capture.</li> </ul> <p><u>NEGATIVE TEST</u></p> <ul style="list-style-type: none"> <li>Send traffic that does not match the configured ACL.</li> <li>Verify that there were no specific logs generated related to matching ACLs.</li> <li>Verify that the packets were not byPassed via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should be able to implement rules for dropping a packet, encrypting a packet and allowing a packet to flow in plaintext.</li> <li>Packet capture of each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. This meets the testing requirements.

#### 6.49 FCS\_IPSEC\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Create ACL with overlapping rules. This ACL permits a subset of traffic and denies a large set of traffic.</li> <li>Apply access list to connection.</li> </ul> <p>Positive Test</p> <ul style="list-style-type: none"> <li>Try to establish connection with ping.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify logs on the TOE.</li> <li>• Verify the connection via packet capture.</li> </ul> <p>Negative Test</p> <ul style="list-style-type: none"> <li>• Try to establish connection with ping.</li> <li>• Verify logs on the TOE.</li> <li>• Verify the connection via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a second set of overlapping rules. This ACL permits a large set of traffic and denies a subset of traffic.</li> <li>• Apply access list to connection.</li> </ul> <p>Positive Test</p> <ul style="list-style-type: none"> <li>• Try to establish connection with ping.</li> <li>• Verify logs on the TOE.</li> <li>• Verify the connection via packet capture.</li> </ul> <p>Negative Test</p> <ul style="list-style-type: none"> <li>• Try to establish connection with ping.</li> <li>• Verify logs on the TOE.</li> </ul> <p>Verify the connection via packet capture.</p>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to permit/deny/byPass the traffic in sequence when configured.</li> <li>• Packet capture of traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. This meets the testing requirements.

### 6.50 FCS\_IPSEC\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches the rule to allow the packet to flow in plaintext and send that packet. The evaluator should observe that the network packet is Passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet and observes that the packet was dropped.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create an ACL to bypass the traffic.</li> <li>• Apply the ACL on the crypto map.</li> <li>• Apply the ACL on the interface.</li> <li>• Attempt to establish a connection and verify that it is bypassing.</li> <li>• Verify via logs that the traffic was bypassed using the ACL.</li> <li>• Verify via packet capture that the packets are bypassed.</li> <li>• Ping the device with modified header containing an IP that is outside of the access lists (192.168.0.104).</li> <li>• Verify via packet capture that the packets are dropped, and the connection fails.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to drop packets with modified header.</li> <li>• Logs, CLI output, and packet captures showing failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When the modified packet is sent, the TOE rejects the connection. This meets the testing requirements.

### 6.51 FCS\_IPSEC\_EXT.1.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	If tunnel mode is selected, the evaluator uses the guidance documentation to configure the TOE to operate in tunnel mode and also configures a VPN peer to operate in tunnel mode. The evaluator configures the TOE and the VPN peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
<b>Test Steps</b>	<p><b>IKEv1</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES-CBC-128 for using SHA1 with tunnel mode</li> <li>• Configure the Peer to use AES-CBC-128 and hash SHA1 with tunnel mode</li> <li>• Generate traffic to trigger the IPsec session</li> <li>• Verify traffic sent is secured using the specified algorithms via log</li> <li>• Verify traffic sent is secured using the specified algorithms via packet capture</li> </ul> <p><b>IKEv2</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES-CBC-256 for using SHA256 with tunnel mode</li> <li>• Configure the Peer to use AES-CBC-256 and hash SHA256 with tunnel mode</li> <li>• Generate traffic to trigger the IPsec session</li> <li>• Verify traffic sent is secured using the specified algorithms via log</li> <li>• Verify traffic sent is secured using the specified algorithms via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should perform a successful connection using tunnel mode.</li> <li>• Log showing that the IPSEC session was in tunnel mode.</li> <li>• Packet capture showing session was in tunnel mode.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to be configured tunnel mode. This meets the testing requirements.

### 6.52 FCS\_IPSEC\_EXT.1.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: If transport mode is selected, the evaluator uses the guidance documentation to configure the TOE to operate in transport mode and also configures a VPN peer to operate in transport mode. The evaluator configures the TOE and the VPN peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.
<b>Test Steps</b>	<p><b>IKEv1</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES-CBC-128 for using SHA1 with transport mode</li> <li>• Configure the Peer to use AES-CBC-128 and hash SHA1 with transport mode</li> <li>• Generate traffic to trigger the IPsec session</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify traffic sent is secured using the specified algorithms via log</li> <li>• Verify traffic sent is secured using the specified algorithms via packet capture</li> </ul> <p><b>IKEv2</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES-CBC-256 for using SHA256 with transport mode</li> <li>• Configure the Peer to use AES-CBC-256 and hash SHA256 with transport mode</li> <li>• Generate traffic to trigger the IPsec session</li> <li>• Verify traffic sent is secured using the specified algorithms via log</li> <li>• Verify traffic sent is secured using the specified algorithms via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should perform a successful connection using transport mode.</li> <li>• Log showing that the IPSEC session was in transport mode.</li> <li>• Packet capture showing session was in transport mode.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to be configured transport mode. This meets the testing requirements.

### 6.53 FCS\_IPSEC\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the TOE as indicated in the guidance documentation configuring the TOE to use each of the supported algorithms, attempt to establish a connection using ESP, and verify that the attempt succeeds.
<b>Test Steps</b>	<p><b><u>IKEV2</u></b></p> <p><b><u>AES-CBC-128 and SHA1</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-CBC-128 and HMAC-SHA1 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-CBC-128 and SHA1.</li> </ul> <p><b><u>AES-CBC-192 and SHA256</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-CBC-192 and HMAC-SHA256 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-CBC-192 and SHA256.</li> </ul> <p><b><u>AES-CBC-256 and Sha512</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-CBC-256 and HMAC-SHA512 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-CBC-256 and SHA512.</li> </ul> <p><b><u>AES-GCM-128</u></b></p> <ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-GCM-128 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-GCM-128 .</li> </ul> <p><b><u>AES-GCM-192</u></b></p>

	<ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-GCM-192 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-GCM-128.</li> </ul> <p><b>AES-GCM-256</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE and IPSEC Peer with AES-GCM-256 configuration in ESP.</li> <li>• Start an IPSEC connection (use Ping command).</li> <li>• Verify via logs and packet capture that the connection was established using AES-GCM-256.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• IPSEC SAs should be configured with each claimed encryption and hash algorithm.</li> <li>• Log showing that the IPSEC session was in claimed encryption and hash algorithm.</li> <li>• Packet capture showing session was in claimed encryption and hash algorithm.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. IPsec SAs can be configured with each claimed encryption algorithm. IPsec SAs can be configured with each claimed hash algorithm. This meets the testing requirements.

#### 6.54 FCS\_IPSEC\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	If <b>IKEV1</b> is selected, the evaluator shall configure the TOE as indicated in the guidance documentation and attempt to establish a connection using an IKEV1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to support IKEV1 using main mode only.</li> <li>• Configure peer for aggressive mode.</li> <li>• Attempt to establish an IPSEC session. (Note the ping does not go through).</li> <li>• Verify that Aggressive mode connections are not possible via log.</li> <li>• Verify that Aggressive mode connections are not possible via packet capture.</li> <li>• Configure the PEER to support IKEV1 using main mode only.</li> <li>• Configure the TOE to support IKEV1 using main mode only.</li> <li>• Attempt to establish an IPSEC session via ping.</li> <li>• Verify that main mode is established in the IPSEC connection via log.</li> <li>• Verify that main mode is established in the IPSEC connection via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject a connection attempt with aggressive mode and then accept a connection attempt with main mode.</li> <li>• Log showing the unsuccessful and successful session attempt.</li> <li>• Packet capture of the unsuccessful and successful session attempt.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejected a connection attempt with Aggressive mode and then accepted a connection attempt with main mode. This meets the testing requirements.

#### 6.55 FCS\_IPSEC\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	If <b>NAT traversal</b> is selected within the IKEV2 selection, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPSEC connection and determine that the NAT is successfully traversed.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE for NAT Traversal.</li> </ul>

	<ul style="list-style-type: none"> <li>• Generate traffic.</li> <li>• Verify that NAT Traversal is performed.</li> <li>• Verify establishment of session via logs from TOE.</li> <li>• Verify NAT traversal occurred via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should perform a successful connection with NAT Traversal.</li> <li>• Log showing the successful session attempt.</li> <li>• Packet capture of the successful session attempt</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. This test case shows that when a peer configured for NAT traversal attempts to initiate an IPsec session with the TOE the NAT is traversed.

### 6.56 FCS\_IPSEC\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEV1 and/or IKEV2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.
<b>Test Steps</b>	<p><b>IKEV1</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE for IKEV1 AES-CBC-128 &amp; SHA-1, Group 14 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify via logs that the connection was established using AES-CBC-128 &amp; SHA-1, Group 14.</li> <li>• Verify via packet capture that the connection was established using AES-CBC-128 &amp; SHA-1, Group 14.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for IKEV1 AES-CBC-192 &amp; SHA-256, Group 15 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify via logs that the connection was established using AES-CBC-192 &amp; SHA256, Group 15.</li> <li>• Verify via packet capture that the connection was established using AES-CBC-192 &amp; SHA256, Group 15.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for IKEV1 AES-CBC-256 &amp; SHA-512, Group 19 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify via logs that the connection was established using AES-CBC-192 &amp; SHA256, Group 19.</li> <li>• Verify via packet capture that the connection was established using AES-CBC-256 &amp; SHA-512, Group 19.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for IKEV1 AES-CBC-128, SHA-1, Group-20 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify via logs that the connection was established using AES-CBC-128 &amp; SHA-1 &amp; Group-20.</li> <li>• Verify via packet capture that the connection was established using AES-CBC-128 &amp; SHA-1 &amp; Group-20.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for IKEV1 AES-CBC-192 &amp; SHA-256 &amp; group 24 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> </ul>



- Verify via logs that the connection was established using AES-CBC-128 & SHA-1 & group 24.
- Verify via packet capture that the connection was established using AES-CBC-128 & SHA-1 & group 24.

## **IKEV2**

- Configure the TOE for IKEV2 AES-CBC-128 & SHA-1 & group 14 configuration.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-CBC-128 & SHA-1 & group 14.
  - Verify via packet capture that the connection was established using AES-CBC-128 & SHA-1 & group 14.
- 
- Configure the TOE for IKEV2 AES-CBC-192 & SHA-256 & group 15 configuration.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-CBC-192 & sha-256 & group 15.
  - Verify via packet capture that the connection was established using AES-CBC-192 & sha-256 & group 15.
- 
- Configure the TOE for IKEV2 AES-CBC-256 & SHA-512 & group 19 configuration in the ESP.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-CBC-256 & SHA512 & group 19.
  - Verify via packet capture that the connection was established using AES-CBC-256 & SHA512 & group 19.
- 
- Configure the TOE for IKEV2 AES-GCM-128 & SHA-1 & group 20 configuration.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-GCM-128 & SHA-1 & group 20.
  - Verify via packet capture that the connection was established using AES-GCM-128 & SHA-1 & group 20.
- 
- Configure the TOE for IKEV2 AES-GCM-128 & SHA-1 & group 20 configuration.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-GCM-128 & SHA-1 & group 20.
  - Verify via packet capture that the connection was established using AES-GCM-128 & SHA-1 & group 20.
- 
- Configure the TOE for IKEV2 AES-GCM-192 & SHA-256 & group 24 configuration.
  - Start an IPSEC connection (using Ping).
  - Verify via logs that the connection was established using AES-GCM-256 & sha-256 & group 24.
  - Verify via packet capture that the connection was established using AES-GCM-256 & SHA-256 & group 24.



	<ul style="list-style-type: none"> <li>• Configure the TOE for IKEV2 AES-GCM-256 &amp; SHA-512 &amp; group 24 configuration.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify via logs that the connection was established using AES-GCM-256 &amp; sha-256 &amp; group 24.</li> <li>• Verify via packet capture that the connection was established using AES-GCM-256 &amp; SHA-256 &amp; group 24.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• IKE SAs should be configured with each claimed ciphersuite.</li> <li>• Log showing that the IKE session was in claimed ciphersuite.</li> <li>• Packet capture showing IKE session was in claimed ciphersuite</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. IKE SAs can be configured with each claimed algorithm. This meets the testing requirements.

### 6.57 FCS\_IPSEC\_EXT.1.7 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: If ' <b>number of bytes</b> ' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 1 negotiation.
<b>Pass/Fail with Explanation</b>	Pass. NA, as the selection 'number of bytes' is not selected.

### 6.58 FCS\_IPSEC\_EXT.1.7 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is performed no later than 24h). The evaluator shall verify that the guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.</p> <p>Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 1 SA lifetime that exceeds the Phase 1 SA lifetime on the TOE.</p> <p><b>TD0633 has been applied</b></p>
<b>Test Steps</b>	<p><u>IKEV1</u></p> <ul style="list-style-type: none"> <li>• Configure the TOE to have lifetime of less than 23.45 hours (85500 sec).</li> </ul>

	<ul style="list-style-type: none"> <li>• Configure the Peer to have lifetime of 24 hours (86400 sec).</li> <li>• Start a connection through the TOE and maintain the connection.</li> <li>• Verify the lifetime from the output of command 'show crypto isakmp sa detail'.</li> <li>• Output of show log on TOE verifies the rekey.</li> </ul> <p><u>IKEV2</u></p> <ul style="list-style-type: none"> <li>• Configure the TOE to have lifetime of less than 23.45 hours (85500 sec).</li> <li>• Configure the Peer to have lifetime of 24 hours (86400 sec).</li> <li>• Start a connection through the TOE and maintain the connection.</li> <li>• Verify the lifetime from the output of command 'show crypto ikev2 sa'.</li> <li>• Output of show log on TOE verifies the rekey.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should renegotiate phase 1 after the lifetime exceeds the configured lifetime of the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE initiated a rekey before the configured time limit. This meets the testing requirements.

### 6.59 FCS\_IPSEC\_EXT.1.8 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: If 'number of bytes' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 2 negotiation.
<b>Test Steps</b>	<p>IKEV1</p> <ul style="list-style-type: none"> <li>• Configure IPSEC on the TOE to have lifetime of 2560 kilobytes.</li> <li>• Configure IPSEC on the Peer to have lifetime of 3000 kilobytes.</li> <li>• Start a connection from the TOE and send enough data to trigger the limit.</li> <li>• Verify the rekey occurred via logs.</li> <li>• Verify the rekey occurred via packet capture.</li> </ul> <p>IKEV2</p> <ul style="list-style-type: none"> <li>• Configure IPSEC on the TOE to have lifetime of 2560 kilobytes.</li> <li>• Configure IPSEC on the Peer to have lifetime of 3000 kilobytes.</li> <li>• Start a connection from the TOE and send enough data to trigger the limit.</li> <li>• Verify the rekey occurred via logs.</li> <li>• Verify the rekey occurred via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should initiate a new SA when the allowed number of bytes through the existing SA is exceeded.</li> <li>• Packet capture showing threshold is met.</li> <li>• Packet capture/logs showing session rekey.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE initiates a rekey when the configured byte interval is exceeded. This meets the testing requirements.

### 6.60 FCS\_IPSEC\_EXT.1.8 Test #2

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the guidance documentation allows the Administrator to configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.</p> <p>Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime no later than 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 2 SA lifetime that exceeds the Phase 2 SA lifetime on the TOE.</p> <p><b>TD0633 has been applied</b></p>
<b>Test Steps</b>	<p>IKEV1</p> <ul style="list-style-type: none"> <li>• Configure IPSEC on the TOE to have lifetime of 7.45hours (26820sec).</li> <li>• Configure IPSEC on the Peer to have lifetime of 8 hours (28800 sec).</li> <li>• Start a connection through the TOE and maintain the connection.</li> <li>• Verify the lifetime from the output of command 'show crypto IPSEC sa detail   include remaining key lifetime'.</li> <li>• Output of show log on TOE verifies the rekey.</li> <li>• Verify the rekey occurred via Packet Capture.</li> </ul> <p>IKEV2</p> <ul style="list-style-type: none"> <li>• Configure IPSEC on the TOE to have lifetime of 7.45 hours (26820 sec).</li> <li>• Configure IPSEC on the Peer to have lifetime of 8 hours 28800 sec).</li> <li>• Start a connection through the TOE and maintain the connection.</li> <li>• Verify the lifetime from the output of command 'show crypto IPSEC sa detail   include remaining key lifetime'.</li> <li>• Output of show log on TOE verifies the rekey.</li> <li>• Verify the rekey occurred via Packet Capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should renegotiate phase 2 after the lifetime exceeds the configured lifetime of the TOE.</li> <li>• Packet capture showing threshold is met.</li> <li>• Packet capture/logs showing session rekey.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. This test case shows that when configured for rekey the TOE will rekey at the configured time interval .This meets the testing requirements.</p>

### 6.61 FCS\_IPSEC\_EXT.1.10 Test #1

Item	Data
<b>Test Assurance Activity</b>	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

	If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
<b>Pass/Fail with Explanation</b>	Pass. NA. Test 1 is duplicate assurance activities to FCS_IPSEC_EXT.1.10 TSS 1 and TSS 2. Please refer AAR for the TSS evaluation activities.

### 6.62 FCS\_IPSEC\_EXT.1.10 Test #2

Item	Data
<b>Test Assurance Activity</b>	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:  If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
<b>Pass/Fail with Explanation</b>	Pass. NA. Test 2 is duplicate assurance activities to FCS_IPSEC_EXT.1.10 TSS 1 and TSS 2. Please refer AAR for the TSS evaluation activities.

### 6.63 FCS\_IPSEC\_EXT.1.11 Test #1

Item	Data
<b>Test Assurance Activity</b>	For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.
<b>Test Steps</b>	<p><b>IKEV1</b></p> <ul style="list-style-type: none"> <li>• Configure DH group 14 for IKEV1 on TOE.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify that DH Group 14 was used via log.</li> <li>• Verify that Group 14 is used via capture.</li>   <li>• Configure DH group 15 for IKEV1 on TOE.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify that DH Group 15 was used via log.</li> <li>• Verify that Group 15 is used via capture.</li>   <li>• Configure the TOE for Group 19.</li> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 19 was used via log.</li> <li>• Verify that DH Group 19 was used via packet capture.</li>   <li>• Configure the TOE for Group 20.</li> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 20 was used via log.</li> <li>• Verify that DH Group 20 was used via packet capture.</li>   <li>• Configure the TOE for Group 24.</li> </ul>

	<ul style="list-style-type: none"> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 24 was used via log.</li> <li>• Verify that DH Group 24 was used via packet capture.</li> </ul> <p><b>IKEV2</b></p> <ul style="list-style-type: none"> <li>• Configure DH group 14 for IKEV1 on TOE.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify that DH Group 14 was used via log.</li> <li>• Verify that Group 14 is used via capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure DH group 15 for IKEV1 on TOE.</li> <li>• Start an IPSEC connection (using Ping).</li> <li>• Verify that DH Group 15 was used via log.</li> <li>• Verify that Group 15 is used via capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for Group 19.</li> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 19 was used via log.</li> <li>• Verify that DH Group 19 was used via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for Group 20.</li> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 20 was used via log.</li> <li>• Verify that DH Group 20 was used via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the TOE for Group 24.</li> <li>• Generate traffic to trigger the IPSEC session.</li> <li>• Verify that DH group 24 was used via log.</li> <li>• Verify that DH Group 24 was used via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• IKE SAs should be configured with each claimed exchange method.</li> <li>• Log showing that the IKE session was in claimed exchange method.</li> <li>• Packet capture showing IKE session was in claimed exchange method.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. This test showed that each of the DH group supported by the TOE was configurable in IPsec connection. This meets the testing requirements.

#### 6.64 FCS\_IPSEC\_EXT.1.12 Test #1

Item	Data
<b>Test Assurance Activity</b>	This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPSEC connection using each of the supported algorithms and hash functions identified in the requirements.
<b>Pass/Fail with Explanation</b>	Pass. This testing is covered by the requirements in FCS_IPSEC_EXT.1.4 Test#1 and FCS_IPSEC_EXT.1.6 Test#1.

### 6.65 FCS\_IPSEC\_EXT.1.12 Test #2

Item	Data
<b>Test Assurance Activity</b>	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure TOE to use AES-CBC-128 in P1 and AES-CBC-128 in P2 IKEV1.</li> <li>• Configure peer to use AES-CBC-128 in P1 and AES-CBC-256 in P2 IKEV1.</li> <li>• Attempt to establish a connection.</li> <li>• Verify the connection is rejected using logs.</li> <li>• Verify the connection is rejected using Packet Capture.</li> </ul> <ul style="list-style-type: none"> <li>• Configure TOE to use AES-CBC-128 in P1 and AES-CBC-128 in P2 IKEV2.</li> <li>• Configure peer to use AES-CBC-128 in P1 and AES-CBC-256 in P2 IKEV2.</li> <li>• Attempt to establish a connection.</li> <li>• Verify the connection is rejected using logs.</li> <li>• Verify the connection is rejected using Packet Capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• When attempting to connect to a peer with the IPSEC SA strength larger than the IKE SA strength, the TOE should be able to reject the connection.</li> <li>• Log showing the failed connection.</li> <li>• Packet capture showing the failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When attempting to connect to a peer with the IPsec SA strength larger than the IKE SA strength. The TOE is able to reject the connection. This meets the testing requirements.

### 6.66 FCS\_IPSEC\_EXT.1.12 Test #3

Item	Data
<b>Test Assurance Activity</b>	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
<b>Test Steps</b>	<p>IKEV1</p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES and SHA1.</li> <li>• Configure the Peer to use 3DES and SHA1.</li> <li>• Attempt a secure IPSEC connection.</li> <li>• Verify the connection is rejected via packet capture.</li> <li>• Verify the logs reflected on the TOE.</li> </ul> <p>IKEV2</p> <ul style="list-style-type: none"> <li>• Configure the TOE to use AES and SHA1.</li> <li>• Configure the Peer to use 3DES and SHA1.</li> <li>• Attempt a secure IPSEC connection.</li> <li>• Verify the connection is rejected via packet capture.</li> <li>• Verify the logs reflected on the TOE.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should only support and propose the configured algorithm. If the TOE peer does not have matching algorithms this session should not be established.</li> </ul>

	<ul style="list-style-type: none"> <li>• Log showing the failed connection.</li> <li>• Packet capture showing the failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE will only support and propose the configured algorithm. If the TOE peer does not have matching algorithms this session will not be established. This meets the testing requirements.

#### 6.67 FCS\_IPSEC\_EXT.1.12 Test #4

Item	Data
<b>Test Assurance Activity</b>	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP (assumes the proper parameters were used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.
<b>Test Steps</b>	<p>IKEV1</p> <ul style="list-style-type: none"> <li>• Configure TOE to support AES-CBC-128 in transform set.</li> <li>• Configure Peer to support 3Des in Transform set.</li> <li>• Attempt a connection between TOE and Peer.</li> <li>• Verify using logs.</li> <li>• Verify the connection is rejected using Packet Capture.</li> </ul> <p>IKEV2</p> <ul style="list-style-type: none"> <li>• Configure TOE to support AES-CBC-128 (P1 and P2).</li> <li>• Configure Peer to support AES-CBC-128 (P1) and 3des-CBC (P2).</li> <li>• Attempt a connection between TOE and Peer.</li> <li>• Verify using logs.</li> <li>• Verify the connection is rejected using Packet Capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Since the IPSEC SA parameters does not match the IPSEC SA parameters of the TOE peer, an IPSEC connection should not be established. An IKE SA, however, should be established because the peer parameters match.</li> <li>• Log showing the failed connection.</li> <li>• Packet capture showing the failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Since the IPsec SA parameters of the TOE did not match the IPsec SA parameters of the peer, an IPsec connection could not be established. An IKE SA, however, could be established because the peer parameters matched. This meets the testing requirements.

#### 6.68 FCS\_IPSEC\_EXT.1.14 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: [conditional] For each CN/identifier type combination selected, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.</p> <p>If the TOE prioritizes CN checking over SAN (through explicit configuration of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the SAN so it contains an incorrect identifier of the correct type (e.g. the reference identifier on the TOE is example.com, the CN=example.com, and the SAN: FQDN=otherdomain.com) and verify that IKE authentication succeeds.</p>
<b>Test Steps</b>	<p><b>CN as FQDN</b></p> <ul style="list-style-type: none"> <li>• Create Trustpoints having CN as FQDN.</li> <li>• Authenticate to the CA.</li> </ul>

	<ul style="list-style-type: none"> <li>Repeat the above steps to authenticate the peer.</li> <li>Configure the TOE with the CN as FQDN.</li> <li>Configure the Peer CN to be similar to the TOE.</li> <li>Attempt to establish a connection between the TOE and Peer.</li> <li>Verify that the connection is successful.</li> <li>Verify packet captures.</li> </ul> <p><b>CN as IP address</b></p> <ul style="list-style-type: none"> <li>Create Trustpoints having CN as IP Address.</li> <li>Authenticate to the CA.</li> <li>Repeat the above steps to authenticate the peer.</li> <li>Configure the TOE with the CN as IP address.</li> <li>Configure the Peer CN to be similar to the TOE.</li> <li>Attempt to establish a connection between the TOE and Peer.</li> <li>Verify that the connection is successful.</li> <li>Verify packet captures.</li> </ul> <p><b>CN as user FQDN</b></p> <ul style="list-style-type: none"> <li>Create Trustpoints having CN as user FQDN.</li> <li>Authenticate to the CA.</li> <li>Repeat the above steps to authenticate the peer.</li> <li>Configure the TOE CN with the peer reference identifier as user FQDN.</li> <li>Configure the Peer CN to be similar to the TOE.</li> <li>Attempt to establish a connection between the TOE and Peer.</li> <li>Verify that the connection is successful.</li> <li>Verify packet captures.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should accept connections when CN matches.</li> <li>Logs of IPSEC session configuration</li> <li>Packet capture showing the session establishment.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE accepts connections with CN matches. This meets the testing requirements.

### 6.69 FCS\_IPSEC\_EXT.1.14 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3: [conditional] For each CN/identifier type combination selected, the evaluator shall:</p> <p>a) Create a valid certificate with the CN so it contains the valid identifier followed by '\0'. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the evaluator shall configure the SAN so it matches the reference identifier.</p> <p>b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the CN without the '\0' and verify that IKE authentication fails.</p>
<b>Test Steps</b>	<p><b>CN as FQDN</b></p> <ul style="list-style-type: none"> <li>Configure the TOE with the CN as IP address without the '\0'.</li> <li>Configure the Peer CN to be like the TOE but with the '\0'.</li> <li>Attempt to establish a connection between the TOE and Peer.</li> </ul>



	<ul style="list-style-type: none"> <li>• Verify that the connection failed.</li> <li>• Verify packet captures.</li> </ul> <p><b>CN as IP address</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE with the CN as FQDN without the '\0'.</li> <li>• Configure the Peer CN to be similar to the TOE but with the '\0'.</li> <li>• Attempt to establish a connection between the TOE and Peer.</li> <li>• Verify that the connection failed.</li> <li>• Verify packet captures.</li> </ul> <p><b>CN as user FQDN</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE with the CN as user FQDN without the '\0'.</li> <li>• Configure the Peer CN to be like the TOE but with the '\0'.</li> <li>• Attempt to establish a connection between the TOE and Peer.</li> <li>• Verify that the connection failed.</li> <li>• Verify packet captures.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject connections when CN mismatches.</li> <li>• Logs showing failed connection.</li> <li>• Packet capture showing failed connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connections with CN mismatches. This meets the testing requirements.

#### 6.70 FCS\_IPSEC\_EXT.1.14 Test #5

Item	Data
<b>Test Assurance Activity</b>	Test 5: [conditional] If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE certificate to the distinguished name.</li> <li>• Attempt to establish a connection between the TOE and Peer.</li> <li>• Verify the connection succeeded with the IKE SA.</li> <li>• Verify the connection succeeded via log.</li> <li>• Verify the connection succeeded via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should accept connections when the presented and the reference identifier of the DN match.</li> <li>• Logs showing successful connection.</li> <li>• Packet capture showing successful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE accepts connections when the presented and the reference identifier of the DN match. This meets the testing requirements

#### 6.71 FCS\_IPSEC\_EXT.1.14 Test #6a

Item	Data
<b>Test Assurance Activity</b>	Test 6: [conditional] If the TOE supports <b>DN</b> identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE:
<b>Test Steps</b>	<p>a) Duplicate the CN field, so the otherwise authorized DN contains two identical CNs.</p> <ul style="list-style-type: none"> <li>• Create CA-ROOT, ICA1 and ICA2 on the XCA tool.</li> <li>• Create trustpoint for CA-ROOT and ICA and authenticate them on TOE.</li> </ul>

	<ul style="list-style-type: none"> <li>• Generate CSR on the TOE and sign it using the XCA tool. This creates a certificate with one CN on TOE.</li> <li>• Import the signed certificate on TOE.</li> <li>• Configure IPsec on the TOE.</li> <li>• Create trustpoint for CA-ROOT and ICA2 and authenticate them on Peer.</li> <li>• Generate CSR on the Peer and sign it using the XCA tool. While signing, duplicate the CN field. This creates a certificate with two identical CNs on Peer.</li> <li>• Import the signed certificate on PEER.</li> <li>• Configure IPsec on the Peer.</li> <li>• Attempt to establish a connection between the TOE and Peer.</li> <li>• Verify the connection refused via logs.</li> <li>• Verify the connection via packet capture due to absence of ESP packets.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the connection when presented with a certificate that contains two identical CNs in the DN field.</li> <li>• Logs showing failed connection.</li> <li>• Packet capture showing failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When presented with a certificate that contains two identical CNs in the DN field, the TOE rejects the connection. This meets the testing requirements.

### 6.72 FCS\_IPSEC\_EXT.1.14 Test #6b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 6: If the TOE supports <b>DN</b> identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE:</p> <p>b) Append '\0' to a non-CN field of an otherwise authorized DN.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create CA-ROOT, ICA1 and ICA2 on the XCA tool.</li> <li>• Create trustpoint for CA-ROOT and ICA1 and authenticate them on TOE.</li> <li>• Generate CSR on the TOE and sign it using the XCA tool. This creates a certificate with DN equal to CC on TOE.</li> <li>• Import the signed certificate on TOE.</li> <li>• Configure IPSEC on the TOE.</li> <li>• Create trustpoint for CARoot and ICA2 and authenticate them on Peer.</li> <li>• Generate CSR on the Peer and sign it using the XCA tool. This creates a certificate with DN equal to CC\0 on Peer.</li> <li>• Import the signed certificate on TOE.</li> <li>• Configure IPSEC on the Peer.</li> <li>• Attempt to establish a connection between the TOE and Peer.</li> <li>• Verify the connection refused via logs.</li> <li>• Verify the connection via packet capture due to absence of ESP packets.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the connection when presented with a certificate that has a Null Character appended to a non-CN field of an otherwise authorized DN.</li> <li>• Logs showing failed connection.</li> <li>• Packet capture showing failed connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When presented with a certificate that has a Null Character appended to a non-CN field of an otherwise authorized DN, the TOE rejects the connection. This meets the testing requirements.

### 6.73 FIA\_X509\_EXT.1.1/Rev Test #1a

Item	Data
<b>Test Assurance Activity</b>	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Authenticate the CA certificate.</li> <li>• Authenticate the TOE intermediate certificate.</li> <li>• Authenticate the Peer intermediate certificate.</li> <li>• Generate a CSR and sign it.</li> <li>• Upload the signed certificate into the TOE.</li> <li>• Attempt to establish a connection between the TOE and Peer and verify that the connection is established due to a valid chain of certificates.</li> <li>• Verify that the connection is successful via audit logs.</li> <li>• Verify that the connection is successful via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• When a complete certificate chain is present, the TOE should establish a successful IPsec connection.</li> <li>• Log showing successful connection.</li> <li>• Packet capture showing successful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When a complete certificate trust chain is present, the TOE is able to make a successful IKE/IPsec connection

### 6.74 FIA\_X509\_EXT.1.1/Rev Test #1a(ECDSA)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:</p> <p>a) Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Generate ECDSA Key on TOE.</li> </ul>

	<ul style="list-style-type: none"> <li>• Authenticate the CA certificate.</li> <li>• Authenticate the TOE intermediate certificate.</li> <li>• Authenticate the Peer intermediate certificate.</li> <li>• Generate a CSR and sign it.</li> <li>• Upload the signed certificate into the TOE.</li> <li>• Attempt to establish a connection between the TOE and Peer and verify that the connection is established due to a valid chain of certificates.</li> <li>• Verify that the connection is successful via audit logs.</li> <li>• Verify that the connection is successful via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• When a complete certificate chain is present, the TOE should establish a successful IPsec connection.</li> <li>• Log showing successful connection.</li> <li>• Packet capture showing successful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When a complete certificate trust chain is present, the TOE is able to make a successful IKE/IPsec connection.

### 6.75 FIA\_X509\_EXT.1.1/Rev Test #1b

Item	Data
<b>Test Assurance Activity</b>	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Delete an intermediate certificate</li> <li>• Attempt to establish a connection between the TOE and Peer and verify that the connection is not established due to an invalid chain of certificates</li> <li>• Verify that the connection fails via audit logs</li> <li>• Verify that the connection failed via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• When an incomplete certificate chain is present, the TOE should not establish an IPsec connection.</li> <li>• Log showing unsuccessful connection.</li> <li>• Packet capture showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When an incomplete certificate trust chain is present, the TOE is not able to make a successful IKE/IPsec connection.

### 6.76 FIA\_X509\_EXT.1.1/Rev Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Change the current date and time on the TOE so certificate goes invalid.</li> <li>• Attempt to make a connection and verify it is failed.</li> <li>• Verify the failure using Packet Capture.</li> <li>• Verify that the certificate is not valid using logs.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should deny the IPsec connection when the certificate is expired.</li> <li>• Log showing unsuccessful connection.</li> <li>• Packet capture showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE denied the connection because of the expired certificate. This meets the testing requirements.

### 6.77 FIA\_X509\_EXT.1.1/Rev Test #3(CRL)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 3: The evaluator shall test that the TOE can properly handle revoked certificates—conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.</p> <p>Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.</p>
<b>Test Steps</b>	<p><b>CRL</b></p> <ul style="list-style-type: none"> <li>• Configure the trustpoint for CA and authenticate the certificate</li> <li>• Configure the trustpoint for intermediate CA and authenticate the certificate</li> <li>• Enroll the CSR and import the toe certificate</li> <li>• Attempt to make a connection via ping (connection will Pass)</li> <li>• Verify the reason via logs</li> <li>• Verify the reason via packet capture</li> <li>• Revoke the peer leaf certificate</li> <li>• Attempt to make a connection via ping (connection will fail)</li> <li>• Verify the reason for failure via logs</li> <li>• Verify via packet capture that the connection failed</li> <li>• Revoke the peer intermediate certificate</li> <li>• Attempt to make a connection via ping (connection will fail)</li> <li>• Verify the reason for failure via logs</li> <li>• Verify via packet capture that the connection failed</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the IPsec connection when either the intermediate certificate or the server certificate has been revoked.</li> <li>• Log showing successful/unsuccessful connection.</li> <li>• Packet capture showing successful/unsuccessful connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not communicate with peers that either have a revoked certificate or one of their intermediate CA certificates are revoked. When presented non-revoked certificates, the TOE accepts the certificate. This meets the testing requirements.

### 6.78 FIA\_X509\_EXT.1.1/Rev Test #4(CRL)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the CRLsign key usage bit set and verify that validation of the CRL fails.</p>
<b>Test Steps</b>	<p><b>CRL</b></p> <ul style="list-style-type: none"> <li>• Configure the trustpoint for Root CA and authenticate.</li> <li>• Configure the trustpoint for peer intermediate CA and authenticate.</li> <li>• Verify that intermediate CA does not have CRL Sign parameter in Key Usage section.</li> <li>• Enroll CSR on the TOE and import it.</li> <li>• Configure IPsec on the TOE.</li> <li>• Attempt a connection with the peer (will fail).</li> <li>• Verify the reason for failure via logs.</li> <li>• Verify the same via Packet Capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the IPsec connection when CA signing the CRL does not have the CRLsign key usage bit set.</li> <li>• Evidence (screenshot or CLI output) showing addition of certificates.</li> <li>• Log showing unsuccessful connection.</li> <li>• Packet capture showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The TOE rejected the CRL when CA signing the CRL to use a signing certificate that does not have the cRLsign key usage bit set. This meets the testing requirements.</p>

### 6.79 FIA\_X509\_EXT.1.1/Rev Test #5

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:</p> <p>The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Authenticate the CA certificate on the TOE.</li> <li>• Authenticate the intermediate certificate on the TOE.</li> <li>• Generate a CSR and import the signed certificate on the TOE.</li> <li>• Configure the IPsec policy on strongswan.</li> <li>• Initiate an IPsec connection modifying a byte in the first 8 bytes of the certificate.</li> <li>• TOE Status shows that no SA were established.</li> </ul>

	<ul style="list-style-type: none"> <li>• TOE Logs show the negotiation failing due to a certificate decoding error.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the IPsec connection when the first byte of the certificate is modified.</li> <li>• Evidence (screenshot or CLI output) showing modification of certificate.</li> <li>• Log showing unsuccessful connection.</li> <li>• Packet capture showing unsuccessful connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connections when the first byte of the certificate is modified. This meets the testing requirements.

### 6.80 FIA\_X509\_EXT.1.1/Rev Test #6

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:</p> <p>Test 6: The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Initiate an IPsec connection modifying the last byte of the certificate. The TOE rejected the certificate so the connection failed.</li> <li>• TOE Logs show the negotiation failed.</li> <li>• Verify the connection failed via Packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the IPsec connection when the byte in the certificate SignatureValue field is modified.</li> <li>• Evidence (screenshot or CLI output) showing modification of certificate.</li> <li>• Log showing unsuccessful connection. Packet capture showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connections when the last byte in the certificate SignatureValue field is modified. This meets the testing requirements.

### 6.81 FIA\_X509\_EXT.1.1/Rev Test #7

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates.</p>



	<p>For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:</p> <p>Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Initiate an IPsec connection modifying the last byte of the certificate. The TOE rejected the certificate, so the connection failed.</li> <li>• TOE Logs show the negotiation failed.</li> <li>• Verify the connection failed via Packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the IPsec connection when the public key of the certificate is modified.</li> <li>• Evidence (screenshot or CLI output) showing modification of certificate.</li> <li>• Log showing unsuccessful connection.</li> <li>• Packet capture showing unsuccessful connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connections when the public key of the certificate is modified. This meets the testing requirements.

### 6.82 FIA\_X509\_EXT.1.1/Rev Test #8a

Item	Data
<b>Test Assurance Activity</b>	<p><b>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</b>  <b>(Conditional on support for a minimum certificate path length of three certificates)</b>  <b>(Conditional on TOE ability to process CA certificates presented in certificate message)</b></p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	Pass. NA, as the TOE is not able to process CA/ICA certificates presented in the certificate message and it is mandatory to CA/ICA must present in Truststore.

### 6.83 FIA\_X509\_EXT.1.1/Rev Test #8b

Item	Data
<b>Test Assurance Activity</b>	<p><b>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</b>  <b>(Conditional on support for a minimum certificate path length of three certificates)</b>  <b>(Conditional on TOE ability to process CA certificates presented in certificate message)</b></p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>



<b>Pass/Fail with Explanation</b>	NA, as the TOE is not able to process CA/ICA certificates presented in the certificate message and it is mandatory to CA/ICA must present in Truststore
-----------------------------------	---

#### 6.84 FIA\_X509\_EXT.1.1/Rev Test #8c

Item	Data
<b>Test Assurance Activity</b>	<p><b>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)</b>  <b>(Conditional on support for a minimum certificate path length of three certificates)</b></p> <p>The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.</p> <p><b>TD0527 (12/1 Update) has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Modified EC-ICA certificate.</li> <li>• Attempt to authenticate an intermediate CA certificate into a TOE's trust store, that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA and observe that it is rejected.</li> <li>• Valid EC-ICA-Certificate</li> <li>• Attempt to authenticate an intermediate CA certificate into a TOE's trust store, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA and observe that it is accepted.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject installation of subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA.</li> <li>• Evidence (screenshot or CLI output) showing installation of the certificates.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE validates the certificate chain when the EC parameter certificate chain is used. This meets the testing requirement.

#### 6.85 FIA\_X509\_EXT.1.2/Rev Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>- a self-signed root CA certificate,</li> <li>- an intermediate CA certificate and</li> <li>- a leaf (node) certificate.</li> </ul> <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p>

	<p>Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ul style="list-style-type: none"> <li>(i) <i>as part of the validation of the leaf certificate belonging to this chain.</i></li> <li>(ii) <i>when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).</i></li> </ul>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a certificate of the CA issuing the TOE's certificate does not contain the Basic Constraints extension.</li> <li>• Verify that the signing CA certificate does not contain the basicConstraints extension.</li> <li>• Attempt to load the certificate; this will fail.</li> <li>• Verify the TOE rejects the certificate via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject certificates signed by CA that does not contain the Basic Constraints Extension.</li> <li>• Evidence (screenshot or CLI output) showing extensions of the certificate.</li> <li>• Log showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. TOE is rejects certificates signed by CA that does not contain the BasicConstraint Extension.

## 6.86 FIA\_X509\_EXT.1.2/Rev Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> <li>- a self-signed root CA certificate,</li> <li>- an intermediate CA certificate and</li> <li>- a leaf (node) certificate.</li> </ul> <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p> <p>Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ol style="list-style-type: none"> <li>1. As part of the validation of the leaf certificate belonging to this chain;</li> <li>2. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).</li> </ol>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a certificate of the CA issuing the TOE's certificate has the CA flag in the Basic Constraints extension set to FALSE.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify that the signing CA certificate has the CA flag in the basic Constraints extension set to FALSE.</li> <li>• Attempt to load the certificate onto the TOE.</li> <li>• Verify the TOE rejects the certificate via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject certificates signed by CA that has CA flag set to FALSE.</li> <li>• Evidence (screenshot or CLI output) showing BasicConstraints of the certificate.</li> <li>• Log showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejects connections when the False CA used to sign a certificate, this meets the testing requirement.

### 6.87 FIA\_X509\_EXT.2 Test #1(CRL)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity.</p> <p>The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed.</p> <p>If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.</p>
<b>Test Steps</b>	<p>CRL</p> <ul style="list-style-type: none"> <li>• Remove CRL list from the CRL server.</li> <li>• Attempt connection. This should fail as CRL cannot verify cert.</li> <li>• Check logs for CRL checking failure.</li> <li>• Verify the connection with packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject certificate when validation checking of the certificate is not available.</li> <li>• Evidence (screenshot or CLI output) showing configuration of CRL.</li> <li>• Log showing successful/unsuccessful connection.</li> <li>• Packet capture showing successful/unsuccessful connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE successfully rejects certificates when validation service is unavailable. This meets the testing requirements.

### 6.88 FIA\_X509\_EXT.3 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• From the TOE, generate a CSR.</li> <li>• Examine the CSR contents. <ul style="list-style-type: none"> <li>○ Ensure the CSR contains the following fields : Public key, CN, Org, OU, Country.</li> </ul> </li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should generate CSR containing the required fields selected in the SFR.</li> <li>Evidence (screenshot or CLI output) showing generation of CSR.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE is able to generate a CSR with all the requisite information. This meets the testing requirements.

### 6.89 FIA\_X509\_EXT.3 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the response message, and demonstrate that the function succeeds.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Configure the CA-ROOT and ICA1 on the TOE.</li> <li>From the TOE, generate a CSR request.</li> <li>Sign the certificate using this CSR and verify that the certificate is signed successfully.</li> <li>Remove the trustpoint for ICA1.</li> <li>Import the certificate without the full trust path. This step will fail.</li> <li>Authenticate ICA1 again and import the certificate. This step will succeed.</li> <li>Validate the certificate's installation.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should not validate a signed CSR if the full trust chain is not present. When a full trust chain is present, the TOE should validate the signed CSR.</li> <li>Evidence (screenshot or CLI output) showing generation of CSR.</li> <li>CLI output showing successful signing of CSR.</li> <li>CLI output showing unsuccessful signing of CSR when the trustpoint is removed</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not install CSR responses signed by a CA without a full trust path. The TOE does install a CSR response signed by a CA with a full trust path. This meets the testing requirements.

### 6.90 FPT\_TST\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>It is expected that at least the following tests are performed:</p> <ol style="list-style-type: none"> <li>Verification of the integrity of the firmware and executable software of the TOE</li> <li>Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.</li> </ol> <p>The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this.</p> <p>For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Turn the device on.</li> <li>Verify correct output of the TOE on demand self-tests.</li> <li>Ensure that the evidence collected from the TOE is correct.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should execute all claimed self-tests during bootup.</li> <li>Evidence (screenshot or CLI output) showing successful self-tests.</li> <li>Log showing the execution of self-tests.</li> </ul>
<b>Pass/Fail with</b>	Pass. The TOE performs all claimed self-tests. This meets the testing requirements.

<b>Explanation</b>	
--------------------	--

### 6.91 FPT\_TUD\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating).</p> <p>The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE.</p> <p>(For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.)</p> <p>After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Show current version</li> <li>• Install new image software</li> <li>• Set TOE to boot to new software &amp; show version before reloading.</li> <li>• Reload device</li> <li>• Check new current version.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support updating into a new software version.</li> <li>• Evidence showing successful updating of the currently installed device image to the new image is to be shown.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to be updated when an image that Passes the integrity test is used. This meets the testing requirements.

### 6.92 FPT\_TUD\_EXT.1 Test #2 (a)

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>1) A modified version (e.g. using a hex editor) of a legitimately signed update.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Verify the version on the TOE.</li> <li>• Modify the image using hex-editor.</li> <li>• Copy the corrupt image on the TOE.</li> <li>• Install the boot image on the TOE and verify that it fails.</li> <li>• Reload the TOE and confirm that the bad image is not installed.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should detect and reject the modified image for software update</li> <li>• Evidence (e.g., screenshot or CLI output) showing old version before and after the update attempt</li> <li>• Evidence showing the failure of the software update</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to detect when an image was corrupted and rejected the image. This meets the testing requirements.

### 6.93 FPT\_TUD\_EXT.1 Test #2 (b)

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>2) An image that has not been signed.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm the version of the TOE.</li> <li>• Remove the signature using hex-editor</li> <li>• Copy new corrupted image.</li> <li>• Verify that after the loading the image on the TOE the version is not changed.</li> <li>• Install boot image on the TOE.</li> <li>• Reload the TOE and Confirm that the bad image cannot be installed.</li> </ul>
	<ul style="list-style-type: none"> <li>• The TOE should detect and reject the image without signature for software update.</li> <li>• Evidence (e.g., screenshot or CLI output) showing old version before and after the update attempt.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.

### 6.94 FPT\_TUD\_EXT.1 Test #2 (c)

Item	Data
<b>Test Assurance Activity</b>	<p>Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature).</p>

<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Confirm the version of the TOE.</li> <li>• Modify the signature using hex-editor.</li> <li>• Copy new corrupted image.</li> <li>• Verify that after the loading the image on the TOE the version is not changed.</li> <li>• Install boot image on the TOE.</li> <li>• Reload the TOE and Confirm that the bad image cannot be installed.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should detect and reject the image with invalid signature for software update.</li> <li>• Evidence (e.g., screenshot or CLI output) showing old version before and after the update attempt.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE software was able to detect when an image had an invalid signature and rejected the image. This meets the testing requirements.

### 6.95 FIA\_PSK\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to support authentication with a 22-character PSK.</li> <li>• Establish a connection to the Peer.</li> <li>• Verify with the help of capture that the connection was successful.</li> <li>• Verify successful connection with the help of logs</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should allow a successful protocol negotiation with a pre-shared key of required characters.</li> <li>• Evidence (screenshot or CLI output) showing configuration of PSK.</li> <li>• Log showing successful authentication.</li> <li>• Packet Capture showing successful authentication.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE allows a successful protocol negotiation with a pre-shared key of required characters. This meets the testing requirement.

### 6.96 FIA\_PSK\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure a 22-character PSK and verify it is accepted.</li> <li>• Configure a maximum length PSK and verify it is accepted.</li> <li>• Configure a PSK of maximum length +1 and verify it cannot be accepted.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should support pre-shared keys of multiple lengths where the minimum and maximum keys are able to perform successful protocol negotiation.</li> <li>• The TOE should reject pre-shared key of length greater than the maximum length.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE accepts keys of lengths within the minimum and maximum length. This meets the testing requirement.



### 6.97 FIA\_PSK\_EXT.1 Test #3

Item	Data
<b>Test Assurance Activity</b>	Test 3 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Provide a bit-based pre-shared key for authentication.</li> <li>• Configure the TOE and Peer for PSK.</li> <li>• Send a ping to the peer device and verify the connection succeeds.</li> <li>• Verify that pre-shared key was used for the negotiation.</li> <li>• Verify the connection via log .</li> <li>• Verify the connection via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should perform a successful protocol negotiation with a bit-based pre-shared key.</li> <li>• Evidence (screenshot or CLI output) showing configuration of PSK.</li> <li>• Log showing successful authentication.</li> <li>• Packet capture showing successful authentication.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE supports the bit-based pre-shared key for successful negotiation. This meets the test requirements.

### 6.98 FAU\_GEN.1/VPN Test #1(MOD\_VPNGW)

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall attempt to flood the TOE with network packets such that the TOE will be unable to process all the packets. This may require the evaluator to configure the TOE to limit the bandwidth the TOE is capable to handling (e.g., use of a 10 MB interface). The evaluator shall then review the audit logs to verify that the TOE correctly records that it is unable to process all of the received packets and verify that the TOE logging behavior is consistent with the TSS.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the Policy Map.</li> <li>• Attempt to send a normal amount of traffic and verify it succeeds.</li> <li>• Attempt to send a large ping request with high size through the tunnel and verify it drops based on the limit.</li> <li>• Verify that the packets were dropped due to policy violation</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should identify packets that are rate limited as the result of a flooded interface.</li> <li>• Evidence (screenshot or CLI output) showing configuration of policy map.</li> <li>• Evidence (screenshot or CLI output) showing policy violation</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE identifies packets that are rate limited as the result of a flooded interface. This meets the testing requirement.

### 6.99 FAU\_GEN.1/VPN Test #2 (MOD\_VPNGW)

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall use a remote VPN client to establish an IPsec session with the TOE and observe that the event is logged in accordance with the expectations of the PP-Module.



<b>Pass/Fail with Explanation</b>	Pass. This test is performed in conjunction with the FCS_IPSEC_EXT.1.1 Test #1. This meets the testing requirements.
-----------------------------------	--

### 6.100 FMT\_SMF.1 Test #1(MOD\_VPNGW)

Item	Data
<b>Test Assurance Activity</b>	The evaluator tests management functions as part of testing the SFRs identified in sections 2.2, 3, and 4. No separate testing for FMT_SMF.1/VPN is required unless one of the management functions in FMT_SMF.1.1/VPN has not already been exercised under any other SFR.
<b>Test Steps</b>	<p><b>FMT_SMF.1.1/VPN</b> The TSF shall be capable of performing the following management functions: [</p> <ul style="list-style-type: none"> <li>• <i>Definition of packet filtering rules;</i></li> <li>• <i>Association of packet filtering rules to network interfaces;</i></li> <li>• <i>Ordering of packet filtering rules by priority;</i></li> <li>• <i>[No other capabilities]].</i></li> </ul>
<b>Expected Test Results</b>	All management functions identified in Security Target should be met by presenting correct test cases
<b>Pass/Fail with Explanation</b>	Per the assurance activity, please refer the Assurance activities for FPF_RUL_EXT.1 for verification of success for this assurance activity.

### 6.101 FPF\_RUL\_EXT.1.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure a filter to drop ICMP traffic.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Verify via log that rule was configured.</li> <li>• Send continual ICMP traffic from a remote system; verify that traffic is dropped while the TOE is running.</li> <li>• Verify that ICMP traffic was denied with logs.</li> <li>• While a continuous ping is running, reboot the TOE.</li> <li>• Verify all traffic was denied.</li> <li>• Verify that ICMP traffic was denied with logs.</li> <li>• Verify with packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should drop traffic while the TOE is being rebooted. The traffic is not processed/sent during bootup.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Evidence (screenshot or CLI output) showing interruption in traffic during reboot.</li> <li>• Log showing denied traffic and interruption in traffic.</li> <li>• Packet capture showing interruption in traffic.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. The TOE did not Pass the traffic during reboot. This meets the testing requirement.
-----------------------------------	---

### 6.102 FPF\_RUL\_EXT.1.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure a filter to permit ICMP traffic.</li> <li>• Apply the filter to the TOE's Interface.</li> <li>• Verify via log that rule was configured.</li> <li>• Send continual ICMP traffic from a remote system; verify that traffic is permitted while the TOE is running.</li> <li>• Verify that ICMP traffic was allowed with logs.</li> <li>• While a continuous ping is running, reboot the TOE and Verify traffic was denied.</li> <li>• Verify through logs.</li> <li>• Verify through a packet capture that all traffic is denied when the TOE is performing a reboot but once the TOE is operational all traffic is allowed</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should drop traffic while the TOE is being rebooted. The traffic is not processed/sent during bootup.</li> <li>• The TOE should only permit traffic through once initialization is complete.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Evidence (screenshot or CLI output) showing interruption in traffic during reboot.</li> <li>• Log showing permitted traffic and interruption in traffic.</li> <li>• Packet capture showing interruption in traffic</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. This requirement Passes as packets that would otherwise be allowed by the ruleset are not permitted through the TOE during initialization.

### 6.103 FPF\_RUL\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall use the instructions in the operational guidance to test that packet filter rules can be created that permit, deny, and log packets for each of the following attributes:</p> <ul style="list-style-type: none"> <li>• IPv4 <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Protocol</li> </ul> </li> <li>• IPv6 <ul style="list-style-type: none"> <li>○ Source address</li> <li>○ Destination Address</li> <li>○ Next Header (Protocol)</li> </ul> </li> <li>• TCP <ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> </li> <li>• UDP</li> </ul>

	<ul style="list-style-type: none"> <li>○ Source Port</li> <li>○ Destination Port</li> </ul> <p>Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Use the CLI to create an ip access-list with rules for IP, ICMP, TCP and UDP. Each of the rules must be accepted by the CLI.</li> <li>• Verify that configuration is logged.</li> <li>• Use the CLI to create an ipv6 access-list with rules for IPv6, ICMPv6, TCP and UDP. Each of the rules must be accepted by the CLI.</li> <li>• Verify that configuration is logged.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should discard, accept, and log traffic according to the configured ruleset. Each of the rules for IP and IPv6 access-lists should be accepted by the TOE.</li> <li>• Evidence (screenshot or CLI output) showing configuration of the ACLs.</li> <li>• Log showing configuration of the ACL rules.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Each of the rules for IP and IPv6 access-lists were accepted by the CLI. This meets the testing requirement.

#### 6.104 FPF\_RUL\_EXT.1.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall repeat Test 1 above for each distinct network interface type supported by the TOE to ensure that Packet filtering rules can be defined for each all-supported type.</p> <p>Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the protocol/attribute combinations required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Display the interfaces on the TOE.</li> <li>• Create an ip access-list with a single rule.</li> <li>• Assign the access list to an Ethernet interface.</li> <li>• Verify that configuration changes are logged.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should accept commands to associate access lists with Ethernet interfaces.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL and assigning it on an interface.</li> <li>• Log showing configuration of the rules.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. Commands to associate access lists with Ethernet interfaces were accepted by the CLI. This meets the testing requirement.
-----------------------------------	---

### 6.105 FPF\_RUL\_EXT.1.5 Test #1


Item	Data
<b>Test Assurance Activity</b>	Test 1: The evaluator shall devise two equal Packet Filtering rules with alternate operations – permit and deny. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure a filter to allow and drop ICMP packets with the allow rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send ICMP traffic.</li> <li>• Verify through logs that traffic is allowed.</li> <li>• Verify allowed traffic via packet capture.</li> <li>• Configure a filter to drop and allow ICMP packets with the drop rule being first.</li> <li>• Apply the filter to the TOE Interface.</li> <li>• Send ICMP traffic.</li> <li>• Verify through logs that traffic is denied.</li> <li>• Verify discarded traffic via packet capture</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should filter traffic based on the order of the ACL configured. When configured with the permit rule first, the traffic is allowed to Pass. When configured with the deny rule first, the traffic is not allowed to Pass.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL and assigning it on an interface.</li> <li>• Log showing behavior of traffic.</li> <li>• Packet capture showing behavior of traffic</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When configured with the permit rule first, traffic is allowed to Pass. When configured with the deny rule first traffic is not allowed to Pass. This meets the requirements.

### 6.106 FPF\_RUL\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure an ACL with one being a subset of the other with “permit” being the first and “deny” being second</li> <li>• Apply filter to the TOE interface</li> <li>• Generate traffic that will trigger the permit rule via log</li> <li>• Show the ACL hits in the log</li> <li>• Show via packet capture taken on Test VM1 that the traffic was permitted</li> <li>• Configure an ACL with one being a superset of the other with “permit” being the first and “deny” being second</li> </ul>

	<ul style="list-style-type: none"> <li>• Apply filter to the TOE interface</li> <li>• Generate the same traffic as before</li> <li>• Show the ACL hits in the log</li> <li>• Show via packet capture taken on Test VM1 that the traffic was permitted</li> </ul> <ul style="list-style-type: none"> <li>• Configure an ACL with one being a subset of the other with “deny” being the first and “permit” being second</li> <li>• Apply filter to the TOE interface</li> <li>• Generate traffic that will trigger the deny rule</li> <li>• Show the ACL hits in the log</li> <li>• Show via packet capture taken on Test VM1 that the traffic was denied</li> </ul> <ul style="list-style-type: none"> <li>• Configure an ACL with one being a superset of the other with “deny” being the first and “permit” being seconds</li> <li>• Apply filter to the TOE interface</li> <li>• Generate the same traffic as before</li> <li>• Show the ACL hits in the log</li> <li>• Show via packet capture taken on Test VM1 that the traffic was denied</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should filter traffic based on the order of the ACL configured. The first rule should be enforced regardless of the specificity of the rule.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL and assigning it on an interface.</li> <li>• Log showing behavior of traffic.</li> <li>• Packet capture showing behavior of traffic.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The evaluator devised two rules such that one is a subset of the other and ensured that the first is enforced regardless of the specificity of the rule.


### 6.107 FPF\_RUL\_EXT.1.6 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after Passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p style="text-align: center;">             IP Transport layer protocols.xlsx         </p> <p>Table of protocols:  <b>TD0597 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create permit rules for each defined IPv4 protocol (1 – 100) “permit without wildcards.”</li> <li>• Apply the rules to a TOE interface.</li> <li>• Generate traffic to hit each ACL rule.</li> <li>• Show that each ACL rule was hit by the traffic.</li> </ul>

	<ul style="list-style-type: none"> <li>• Show log of each traffic match.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul> <ul style="list-style-type: none"> <li>• Create permit rules for each defined IPv4 protocol (1 – 100) “permit with wildcard destination”.</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul> <ul style="list-style-type: none"> <li>• Create permit rules for each defined IPv4 protocol (1 – 100) “permit with wildcard source”.</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul> <ul style="list-style-type: none"> <li>• Create permit rules for each defined IPv4 protocol (1 – 100) “permit with wildcard both”.</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for permitting each IPV4 traffic flow and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test case showed that a rule can be configured for each of the traffic flow. Each traffic flow was permitted and logged. This meets the requirement.


### 6.108 FPF\_RUL\_EXT.1.6 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the

	<p>supported protocols are denied (i.e., by capturing no applicable packets Passing through the TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.</p> <div style="text-align: center;">         IP Transport layer        protocols.xlsx     </div> <p>Table of protocols:  <b>TD0597 has been applied.</b></p>
<p><b>Test Steps</b></p>	<ul style="list-style-type: none"> <li>• Create deny rules for each defined IPv4 protocol (1 – 100) “deny without wildcards.”</li> <li>• Apply the rules to TOE interface.</li> <li>• Generate traffic to hit each ACL rule.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec bridge.</li>   <li>• Create deny rules for each defined IPv4 protocol (1 – 100) “deny with wildcard destination”.</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec bridge.</li>   <li>• Create deny rules for each defined IPv4 protocol (1 – 100) “deny with wildcard source.”</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec bridge.</li>   <li>• Create deny rules for each defined IPv4 protocol (1 – 100) “deny with wildcard both.”</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec bridge.</li> </ul>
<p><b>Expected Test Results</b></p>	<ul style="list-style-type: none"> <li>• The TOE should create rules for denying each IPV4 traffic flow and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>

<b>Pass/Fail with Explanation</b>	Pass. The test case showed that a rule can be configured for each of the traffic flow. Each traffic flow was denied and logged. This meets the requirement.
-----------------------------------	---


### 6.109 FPF\_RUL\_EXT.1.6 Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets Passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p style="text-align: center;">             IP Transport layer protocols.xlsx         </p> <p>Table of protocols:  <b>TD0597 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a filter to permit traffic with a defined Transport Layer Protocol that contains a specific source address and specific destination address and deny traffic with a defined Transport Layer Protocol that contains a specific source address and specific destination address.</li> <li>• Apply the filter to TOE's interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Verify via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit traffic with a defined Transport Layer Protocol that contains a specific source address and a wildcard destination address and deny traffic with a defined Transport Layer Protocol that contains a specific source address and a wildcard destination address.</li> <li>• Apply the filter to TOE's interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Verify via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit traffic with a defined Transport Layer Protocol that contains a wildcard source address and specific destination address and deny traffic with a defined Transport Layer Protocol that contains a wildcard source address and specific destination address.</li> </ul>



	<ul style="list-style-type: none"> <li>• Apply the filter to TOE's interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Verify via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit traffic with a defined Transport Layer Protocol that contains a wildcard source address and wildcard destination address and deny traffic with a defined Transport Layer Protocol that contains a wildcard source address and wildcard destination address.</li> <li>• Apply the filter to TOE's interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Verify via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should filter traffic based on the order of the ACL configured. When configured with the permit rule first, the traffic is allowed to Pass. When configured with the deny rule first, the traffic is not allowed to Pass.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL and assigning it on an interface.</li> <li>• Log showing behavior of traffic.</li> <li>• Packet capture showing behavior of traffic.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test case showed that a rule can be configured for each of the traffic flow. Each traffic flow was logged and not permitted. This meets the requirement.


#### 6.110 FPF\_RUL\_EXT.1.6 Test #4

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after Passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p style="text-align: center;">             IP Transport layer protocols.xlsx         </p> <p>Table of protocols:  <b>TD0597 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create permit rules for each defined IPv6 protocol (1 – 142) “permit without wildcard.”</li> <li>• Apply the rules to a TOE interface.</li> <li>• Generate traffic to hit each ACL rule.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> </ul>


	<ul style="list-style-type: none"> <li>• Show packet capture of the traffic being Passed taken on Test VM1.</li> <li>• Show packet capture of the traffic being Passed taken on IPsec bridge.</li> <li>• Create permit rules for each defined IPv6 protocol (1 – 142) “permit with wildcard destination”</li> <li>• Apply the ACLs to an interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being Passed taken on Test VM1.</li> <li>• Show packet capture of the traffic being Passed taken on IPsec bridge.</li> <li>• Create permit rules for each defined IPv6 protocol (1 – 142) “permit with wildcard source”.</li> <li>• Apply the ACLs to an interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being Passed taken on Test VM1.</li> <li>• Show packet capture of the traffic being Passed taken on IPsec bridge.</li> <li>• Create permit rules for each defined IPv6 protocol (1 – 142) “permit with wildcard both”.</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being Passed taken on Test VM1.</li> <li>• Show packet capture of the traffic being Passed taken on IPsec bridge.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for permitting each IPV6 traffic flow and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	The test case showed that a rule can be configured for each of the traffic flow. Each traffic flow was denied and logged. This meets the requirement.

### 6.111 FPF\_RUL\_EXT.1.6 Test #5

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets Passing through the

	<p>TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.</p>  <p>IP Transport layer protocols.xlsx</p> <p>Table of protocols: <b>TD0597 has been applied.</b></p>
<p><b>Test Steps</b></p>	<ul style="list-style-type: none"> <li>• Create deny rules for each defined IPv6 protocol (0 – 142) “deny without wildcards.”</li> <li>• Apply the rules to a TOE interface.</li> <li>• Generate traffic to hit each ACL rule.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec Bridge.</li>   <li>• Create deny rules for each defined IPv6 protocol (0 – 142) “deny with wildcard destination”</li> <li>• Apply the ACLs to an interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec Bridge.</li>   <li>• Create deny rules for each defined IPv6 protocol (0 – 142) “Deny with wildcard source”</li> <li>• Apply the ACLs to an interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec Bridge.</li>   <li>• Create deny rules for each defined IPv6 protocol (0 – 142) “deny with wildcard both.”</li> <li>• Apply to interface.</li> <li>• Generate traffic to trigger each ACL.</li> <li>• Show that each ACL rule was hit by the traffic.</li> <li>• Show log of each traffic match.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> <li>• Show packet capture of the traffic being denied taken on IPsec Bridge.</li> </ul>
<p><b>Expected Test Results</b></p>	<ul style="list-style-type: none"> <li>• The TOE should create rules for denying each IPV6 traffic flow and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<p><b>Pass/Fail with Explanation</b></p>	<p>Pass. The test case showed that a rule can be configured for each of the traffic flow. Each traffic flow was denied and logged. This meets the requirement.</p>

### 6.112 FPF\_RUL\_EXT.1.6 Test #6

Item	Data
<p><b>Test Assurance Activity</b></p>	<p>The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are dropped (i.e., by capturing no applicable packets Passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <div style="text-align: center;">  <p>IP Transport layer protocols.xlsx</p> </div> <p>Table of protocols:  <b>TD0597 has been applied.</b></p>
<p><b>Test Steps</b></p>	<ul style="list-style-type: none"> <li>• Create permit and deny rules for each defined IPv6 protocol (1 – 142) without wildcards.</li> <li>• Apply the rules to a TOE interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create permit and deny rules for each defined IPv6 protocol (1 – 142) with wildcard destination.</li> <li>• Apply to interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create permit and deny rules for each defined IPv6 protocol (1 – 142) with wildcard source.</li> <li>• Apply to interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> </ul>

	<ul style="list-style-type: none"> <li>• Create permit and deny rules for each defined IPv6 protocol (1 – 142) with wildcard both.</li> <li>• Apply to interface.</li> <li>• Generate traffic to match the protocol but outside of the source/destination range.</li> <li>• Verify that each ACL rule was not hit by the traffic.</li> <li>• Verify via logs.</li> <li>• Show packet capture of the traffic being denied taken on TestVM1.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should filter traffic based on the order of the ACL configured. When configured with the permit rule first, the traffic is allowed to Pass. When configured with the deny rule first, the traffic is not allowed to Pass.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL and assigning it on an interface.</li> <li>• Log showing behavior of traffic.</li> <li>• Packet capture showing behavior of traffic.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test did not case showed that a rule can be configured for each of the traffic flow. Each traffic flow was not denied and logged. This does not meet the requirement.

### 6.113 FPF\_RUL\_EXT.1.6 Test #7

Item	Data
<b>Test Assurance Activity</b>	Test 7: The evaluator shall configure the TOE to permit and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after Passing through the TOE) and logged.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a filter to permit Transport Layer Protocol 6 using a specific source port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the correct traffic was permitted through the interface.</li> <li>• Verify via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit Transport Layer Protocol 6 using a specific destination port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the correct traffic was permitted through the interface.</li> <li>• Verify via packet capture.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit Transport Layer Protocol 6 using a specific source and destination port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the correct traffic was permitted through the interface.</li> <li>• Verify via packet capture.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for permitting each protocol 6 source and destination ports and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test case showed that when configured TCP traffic can flow through the TOE. This meets the requirements.

#### 6.114 FPF\_RUL\_EXT.1.6 Test #8

Item	Data
<b>Test Assurance Activity</b>	Test 8: The evaluator shall configure the TOE to discard and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets Passing through the TOE) and logged.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a filter to deny Transport Layer Protocol 6 using a specific source port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to deny Transport Layer Protocol 6 using a specific destination port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to deny Transport Layer Protocol 6 using a specific source and destination port.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify the logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for denying each protocol 6 source and destination ports and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test showed that when configured with deny rules TCP traffic will not be permitted. This meets the test case.

### 6.115 FPF\_RUL\_EXT.1.6 Test #9

Item	Data
<b>Test Assurance Activity</b>	Test 9: The evaluator shall configure the TOE to permit and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after Passing through the TOE) and logged. Here the evaluator ensures that the UDP port 500 (IKE) is included in the set of tests.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a filter to permit UDP protocol 17 using a specific source port 500.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was permitted through the interface.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit UDP protocol 17 using a specific destination port 500.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was permitted through the interface.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to permit UDP protocol 17 using a specific source and destination port 500 &amp; 500 respectively.</li> <li>• Apply the filter the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was permitted through the interface.</li> <li>• Verify via packet capture taken Test VM1.</li> <li>• Verify via packet capture taken on IPsec bridge.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for permitting each protocol 17 source and destination ports and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test case showed that when configured UDP traffic can flow through the TOE. This meets the requirements.

### 6.116 FPF\_RUL\_EXT.1.6 Test #10

Item	Data
<b>Test Assurance Activity</b>	Test 10: The evaluator shall configure the TOE to discard and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no

	applicable packets Passing through the TOE) and logged. Again, the evaluator ensures that UDP port 500 is included in the set of tests.
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Create a filter to deny UDP protocol 17 using a specific source port 500.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to deny UDP protocol 17 using a specific destination port 500.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul> <ul style="list-style-type: none"> <li>• Create a filter to drop UDP protocol 17 using a specific source and destination port 500 &amp; 500.</li> <li>• Apply the filter to the TOE's interface.</li> <li>• Generate traffic to match the filters applied to the TOE's interface.</li> <li>• Verify that the traffic hit the configured ACL.</li> <li>• Verify through logs that the traffic was denied through the interface.</li> <li>• Verify via packet capture taken on Test VM1.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should create rules for denying each protocol 17 source and destination ports and log each traffic match.</li> <li>• Evidence (screenshot or CLI output) showing configuration of ACL.</li> <li>• Log showing each traffic match.</li> <li>• Packet capture showing each traffic flow.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The test showed that when configured with deny rules UDP traffic will not be permitted. This meets the test case.

### 6.117 FAU\_GEN.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall complete the assurance activity for FAU_GEN.1 as described in the NDcPP for the auditable events defined above in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this EP are appropriately audited.
<b>Test Steps</b>	Pass. This test is covered by FAU_GEN.1 Test #1 (NDcPP).
<b>Pass/Fail with Explanation</b>	Pass. This test is covered by FAU_GEN.1 Test #1 (NDcPP).

### 6.118 FCS\_MACSEC\_EXT.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment and verify that the TSF logs the



	communications. The evaluator shall capture the traffic between the TOE and the Operational Environment to determine the SCI that the TOE uses to identify the peer. The evaluator shall then configure a test system to capture traffic between the peer and the TOE to modify the SCI that is used to identify the peer. The evaluator then verifies that the TOE does not reply to this traffic and logs that the traffic was discarded. <b>TD0553 has been applied.</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Configure the TOE to use MACsec.</li> <li>• Configure the PEER to use MACsec.</li> <li>• Attempt a connection and verify that it is successful.</li> <li>• Verify that a MKA session is established.</li> <li>• Verify via packet capture.</li> <li>• Verify via logs.</li> <li>• Use MACsec testing tool (acumen-MACsec) to modify SCI of traffic from peer.</li> <li>• Check the PCAP for modified packets and note the lack of reply to packets from TOE.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able establish a successful MACsec channel between the TOE and peer.</li> <li>• Evidence (screenshot or CLI output) of configuring the MACsec.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Successful MACsec connection was established, and during SCI modify test, modified SCI packets were rejected by the TOE. This meets the testing requirements.

#### 6.119 FCS\_MACSEC\_EXT.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall send Ethernet traffic to the TOE's MAC address that iterates through the full range of supported EtherType values (refer to <a href="http://standards.ieee.org/develop/regauth/EtherType/eth.txt">http://standards.ieee.org/develop/regauth/EtherType/eth.txt</a> ) and observes that traffic for all EtherType values is discarded by the TOE except for the traffic which has an EtherType value of 88-8E, 88-E5 or 8808. Note that there are a large number of EtherType values, so the evaluator is encouraged to execute a script that automatically iterates through each value. <b>TD0553 has been applied.</b>
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>• Start the MACsec tool to send the full range of supported ethertypes.</li> <li>• Verify that the packet capture shows various ethertypes sent with NO reply from the TOE.</li> <li>• Verify that the packet capture with etherType 88-8E and 88-E5 or 88-08 are accepted by the TOE.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence of sending a variety of Ether Type .</li> <li>• Packet capture of EtherType sent with NO reply from the TOE.</li> <li>• Packet capture of EtherType 88-8E and 88-E5 or 88-08 accepted by the TOE.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. It is seen from the packet capture that the traffic for all EtherType values is discarded by the TOE except for the traffic which has an EtherType value of 88-8E, 88-E5 or 88-08.

#### 6.120 FCS\_MACSEC\_EXT.2 Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	The evaluator shall transmit MACsec traffic to the TOE from a MACsec-capable peer in the Operational Environment. The evaluator shall verify via packet captures and/or audit logs that the frame bytes after the MACsec Tag values in the received traffic is not obviously predictable.
<b>Test Steps</b>	Acquire Packet Capture of a successful MACsec connection from FCS_MACSEC_EXT.1 Test #1. <ul style="list-style-type: none"> <li>• Verify in Packet Capture that MACsec packets is not obviously predictable.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able establish a successful MACsec channel between the TOE and peer.</li> <li>• Packet Capture showing that frame bytes are not obviously predictable.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Bytes following the MACsec tag in the MKPDUs are not obviously predictable. This meets the testing requirements.

### 6.121 FCS\_MACSEC\_EXT.2 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit valid MACsec traffic to the TOE from a MACsec-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>• Use the MACsec tool to modify a bit in a packet payload.</li> <li>• Verify the Packet Capture for modified packets. Note that no reply from the TOE was detected</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the MACsec connection when a bit in the packet payload is modified.</li> <li>• Evidence (screenshot or CLI output) showing modification of packet.</li> <li>• Packet capture showing before and after modification of payload.</li> <li>• Packet capture showing unsuccessful connection.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Modified ICV packets are rejected by the TOE. This meets the testing requirements.

### 6.122 FCS\_MACSEC\_EXT.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	For each supported method of peer authentication in FCS_MACSEC_EXT.4.1, the evaluator shall follow the operational guidance to configure the supported method (if applicable). The evaluator shall set up a packet sniffer between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then initiate a connection between the TOE and the peer such that authentication occurs, and a secure connection is established. The evaluator shall wait 1 minute and then disconnect the TOE from the peer and stop the sniffer. The evaluator shall use the packet captures to verify that the secure channel was established via the selected mechanism and that the EtherType of the first data frame sent between the TOE and the peer is 88-E5.
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>• Clear the previous MKA sessions and start a new session.</li> <li>• Wait for 1 minute and disconnect the TOE from the peer.</li> </ul>

	<ul style="list-style-type: none"> <li>• Verify from the Packet Capture that the first packet has EtherType of 88-E5.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to create MACsec connection with the peer for 1 minute.</li> <li>• Packet Capture to verify first data packet sent between TOE and peer is 88-E5.</li> <li>• Logs to verify first data packet sent between TOE and peer is 88-E5</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The AES key is wrapped in the captured MKPDUs. This meets the testing requirements

### 6.123 FCS\_MACSEC\_EXT.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall capture traffic between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then cause the TOE to distribute a SAK to that peer, capture the MKPDUs from that operation, and verify the key is wrapped in the captured MKPDUs. <b>TD0273 has been Applied.</b>
<b>Test Steps</b>	Acquire Packet Capture of a successful MACsec connection from FCS_MACSEC_EXT.1 Test #1. <ul style="list-style-type: none"> <li>• Verify in Packet Capture that TOE sends distributed SAK to peer.</li> <li>• Verify in Packet Capture that the key is wrapped in the captured MKPDUs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able establish a successful MACsec channel between the TOE and peer.</li> <li>• Packet Capture showing AES key wrapped in the MKPDUs</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The AES key is wrapped in the captured MKPDUs. This meets the testing requirements

### 6.124 FCS\_MKA\_EXT.1.2 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall use a peer device to send traffic to the TOE, arbitrarily inducing artificial delays in their transmission using a man-in-the-middle setup. The evaluator shall observe that traffic delayed longer than 2.0 seconds is rejected. <b>TD0105 has been applied.</b>
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>• Use the MACsec tool to inject delays into traffic transmission.</li> <li>• Observe the Packet Capture, the delay causes the channel to fail.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should reject the connection when a delay is injected into traffic.</li> <li>• Evidence (screenshot or CLI output) showing injection of delay into traffic transmission.</li> <li>• Packet capture showing session failure.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. After a delay, the MACsec connection broke. This meets the testing requirements.

### 6.125 FCS\_MKA\_EXT.1.4 Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit MKA traffic (MKPDUs) to the TOE from a MKA-capable 21 peer in the Operational Environment. The evaluator shall verify via packet captures and/or audit

	logs that the last 16 octets of the MKPDUs in the received traffic do not appear to be predictable.
<b>Test Steps</b>	Acquire PCAP of a good MACsec connection from FCS_MACSEC_EXT.1 Test #1. <ul style="list-style-type: none"> <li>Observe the last 16 octets of MKA frame in the Packet Capture and verify that they are in an unpredictable sequence.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should be able establish a successful MKA traffic between the TOE and peer.</li> <li>Packet capture showing last 16 octets of MKA frame are in unpredictable sequence</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The last 16 octets of a given MKA frame is in an unpredictable sequence. This meets the testing requirements.

#### 6.126 FCS\_MKA\_EXT.1.4 Test #2

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall transmit valid MKA traffic to the TOE from a MKA-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>Run the MACsec tool to modify a frame byte in transit.</li> <li>Examine the Packet Capture and note how the packet is modified.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should reject the MKA traffic when a bit in the packet payload is modified.</li> <li>Evidence (screenshot or CLI output) showing modification of packet.</li> <li>Packet capture showing before and after modification of payload.</li> <li>Packet capture showing unsuccessful connection</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Modified MKA packets were rejected by the TOE. This meets the testing requirements.

#### 6.127 FCS\_MKA\_EXT.1.5 Test #1

Item	Data
<b>Test Assurance Activity</b>	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic. Test 1: The evaluator shall send a fresh SAK that includes both peers as active participants. The evaluator shall start an MKA session between the TOE and the two active participant peers and send MKPDUs. The evaluator shall verify from packet captures that MKPDUs are sent at least once every half-second. <b>TD0105 has been applied.</b>
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test #1 test case for configuration. <ul style="list-style-type: none"> <li>Clear previous MACsec sessions.</li> <li>Start the MACsec connection with Peer B.</li> <li>Verify from the Packet Capture that the MKA packets are sent every 0.5 seconds.</li> <li>Start the MACsec connection with Peer C</li> <li>Verify from the Packet Capture that the MKA packets are sent every 0.5 seconds.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to send MKPDUs to two active participant peers.</li> <li>• Packet Capture showing the MKPDUs are sent at least once every half-second.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. MKA packets are sent regularly every half a second. This meets the testing requirements.

### 6.128 FCS\_MKA\_EXT.1.5 Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic. Test 2: Disconnect one of the peers. Using a man-in-the-middle device, arbitrarily introduce an artificial delay in sending a fresh SAK following the change in the Live Peer List. Repeat Test 1 delaying a fresh SAK for MKA Lifetime traffic and observe that the timeout of 6.0 seconds is enforced by the TSF.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test #1 test case for configuration.</p> <ul style="list-style-type: none"> <li>• Disconnect one of the peers.</li> <li>• Run the MACsec tool that will delay the distributed SAK file, then restart the MACsec connection.</li> <li>• Examine the Packet Capture. The Test begins at Packet</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of introducing an artificial delay in sending a SAK.</li> <li>• Packet Capture showing a traffic delayed over 6 seconds causing the MACsec connection failure</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Traffic delayed over 6 seconds causes the MACsec connection to fail. This meets the testing requirements.

### 6.129 FCS\_MKA\_EXT.1.8 Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 1: The evaluator shall perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Load one PSK onto the TOE and device B and a second PSK onto the TOE and device C. This defines two pairwise CAs.</li> <li>2. Generate a group CAK for the group of 3 devices using <code>ieee8021XKayCreateNewGroup</code>.</li> <li>3. Observe via packet capture that the TOE distributes the group CAK to the two peers, protected by AES key wrap using their respective PSKs.</li> <li>4. Verify that B can form a SA with C and connect securely.</li> <li>5. Disable the KaY functionality of device C using <code>ieee8021XPaePortKayMkaEnable</code>.</li> <li>6. Generate a group CAK for the TOE and B using <code>ieee8021XKayCreateNewGroup</code> and observe they can connect.</li> </ol>

	<p>7. The evaluator shall have B attempt to connect to C and observe this fails.</p> <p>8. Re-enable the KaY functionality of device C.</p> <p>9. Invoke ieee8021XKeyCreateNewGroup again.</p> <p>10. Verify that both the TOE can connect to C and that B can connect to C.</p> <p><b>TD0105 has been applied.</b></p>
<b>Pass/Fail with Explanation</b>	NA. The TOE does not support group CAKs.

### 6.130 FCS\_MKA\_EXT.1.8 Test #2a

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>1. Send an MKPDU to the TOE's individual MAC address from a peer. Verify the frame is dropped and logged.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test #1 test case for configuration.</p> <ul style="list-style-type: none"> <li>• Use the MACsec tool to send traffic to the individual MAC address of the TOE.</li> <li>• Verify the failure of MKPDU traffic from the MKA statistics.</li> <li>• The PCAP shows that the delivered packet is ignored by the TOE with no reply.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of sending MKA traffic from peer to the individual MAC address of the TOE.</li> <li>• Packet Capture showing a traffic is dropped.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. All modified packets are dropped by TOE. This meets the testing requirements.

### 6.131 FCS\_MKA\_EXT.1.8 Test #2b

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>2. Send an MKPDU to the TOE that is less than 32 octets long. Verify the frame is dropped and logged.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test #1 test case for configuration.</p> <ul style="list-style-type: none"> <li>• Use the MACsec tool to send packets less than 32 octets long.</li> <li>• Verify from Packet Capture that the modified packets are dropped.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of sending MKPDU to the TOE that is less than 32 octets long.</li> </ul>

	<ul style="list-style-type: none"> <li>• Packet Capture showing that the modified packets are dropped.</li> <li>• Logs showing the traffic is dropped</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. MKPDU packets lesser than 32 octets are rejected by the TOE. This meets the testing requirements.

### 6.132 FCS\_MKA\_EXT.1.8 Test #2c

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>3. Send an MKPDU to the TOE whose length in octets is not a multiple of 4. Verify the frame is dropped and logged.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test #1 test case for configuration</p> <ul style="list-style-type: none"> <li>• Use the MACsec tool to send packets whose octets are not a multiple of 4.</li> <li>• Verify from Packet Capture that the modified packets are ignored.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of sending MKPDU to the TOE whose length in octets is not a multiple of 4.</li> <li>• Packet Capture showing that the modified packets are dropped.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. MKPDU sent to the TOE whose length in octets is not a multiple of 4 are dropped by the TOE. This meets the testing requirements.

### 6.133 FCS\_MKA\_EXT.1.8 Test #2d

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>4. Send an MKPDU to the TOE that is one byte short. Verify the frame is dropped and logged.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration.</p> <ul style="list-style-type: none"> <li>• Use the MACsec tool to send MKPDU packets whose length are one byte short.</li> <li>• Verify from Packet Capture that the modified packets are ignored.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of sending MKPDU to the TOE that is one byte short.</li> <li>• Packet Capture showing that the modified packets are dropped.</li> </ul>



<b>Pass/Fail with Explanation</b>	Pass. MKPDU sent to the TOE that is one byte short are dropped by the TOE. This meets the testing requirements.
-----------------------------------	---

### 6.134 FCS\_MKA\_EXT.1.8 Test #2e

Item	Data
<b>Test Assurance Activity</b>	<p>The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests:</p> <p>Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:</p> <p>5. Send an MKPDU to the TOE with unknown Agility Parameter. Verify the frame is dropped and logged.</p> <p><b>TD0105 has been applied.</b></p>
<b>Test Steps</b>	<p>Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration.</p> <ul style="list-style-type: none"> <li>• Use MACsec tool to send MKPDU packet with unknown agility parameters.</li> <li>• Verify the failure of MKPDU traffic from the MKA statistics.</li> <li>• The PCAP shows the modified packets are rejected.</li> <li>• Verify via logs.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of sending MKPDU to the TOE with unknown Agility Parameter.</li> <li>• Packet Capture showing that the modified packets are dropped.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. Packets with unknown Agility Parameter are dropped by the TOE. This meets the testing requirements.

### 6.135 FIA\_AFL.1 Test #1 (MACsec)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE:</p> <p>Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached for a given remote administrator account, subsequent attempts with valid credentials are not successful.</p> <p><b>Note: There is some overlap between the FIA_AFL.1 tests for MACsec and NDcPP.</b></p>
<b>Pass/Fail with Explanation</b>	Pass. This test is covered in FIA_AFL.1 Test #1.

### 6.136 FIA\_AFL.1 Test #2 (MACsec)

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE:</p> <p>Test 2: [conditional] If the TSS indicates that <b>administrative action</b> is necessary to re-enable an account that was locked out due to excessive authentication failures, the evaluator shall perform the steps in Test 1 to lock out an account, follow the operational guidance to manually re-enable the locked-out administrator account, and observe that it is once again able to successfully log in.</p>



	<b>Note: There is some overlap between the FIA_AFL.1 tests for MACsec and NDcPP.</b>
<b>Pass/Fail with Explanation</b>	Pass. This test is covered in FIA_AFL.1 Test #2.

### 6.137 FIA\_PSK\_EXT.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.</p> <p>Test 1 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall use the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.</p>
<b>Test Steps</b>	<p><b>128-bit key</b></p> <ul style="list-style-type: none"> <li>• Attempt to input a 31-character key. This is rejected</li> <li>• Attempt to input a 33-character key. This is rejected</li> <li>• Attempt to input a 32-character key. This is accepted</li> </ul> <p><b>256-bit key</b></p> <ul style="list-style-type: none"> <li>• Attempt to input a 63-character key. This is rejected</li> <li>• Attempt to input a 65-character key. This is rejected</li> <li>• Attempt to input a 64-character key. This is accepted.</li> </ul>
<b>Expected Test Results</b>	The TOE shall successfully negotiate MACsec with the correct key sizes and reject MACsec negotiation attempt with incorrect key sizes.
<b>Pass/Fail with Explanation</b>	Pass. The TOE only supports fixed length pre-shared keys for MACsec.

### 6.138 FIA\_PSK\_EXT.1/MACSEC Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.</p> <p>Test 2 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.</p>
<b>Test Steps</b>	<p><b>128 bits</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use MACsec key-chain with cryptographic algorithm set to aes-128-cmac (32 hex digits).</li> <li>• Configure the Peer to use MACsec key-chain with cryptographic algorithm set to aes-128-cmac (32 hex digits).</li> <li>• Verify the key-chain parameters of the TOE.</li> <li>• Initiate a MACsec connection from the peer.</li> <li>• Verify the connection via packet capture.</li> </ul>

	<p><b>256 bits</b></p> <ul style="list-style-type: none"> <li>• Configure the TOE to use MACsec key-chain with cryptographic algorithm set to aes-256-cmac (64 hex digits).</li> <li>• Configure the Peer to use MACsec key-chain with cryptographic algorithm set to aes-256-cmac (64 hex digits).</li> <li>• Verify the key-chain parameters of the TOE.</li> <li>• Initiate a MACsec connection from the peer.</li> <li>• Verify the connection via packet capture.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should perform a successful protocol negotiation with a bit-based pre-shared key.</li> <li>• Log showing successful authentication.</li> <li>• Packet capture showing successful authentication.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The entered key will be used in a successful MACsec connection. This meets the testing requirements.

### 6.139 FIA\_PSK\_EXT.1/MACSEC Test #3

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.</p> <p>Test 3 [conditional]: If the TOE does <b>generate</b> bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.</p>
<b>Pass/Fail with Explanation</b>	NA. The TOE does not generate bit based pre-shared keys.

### 6.140 FMT\_SMF.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	<p>Test 1: The evaluator shall connect to the PAE of the TOE and install a PSK. The evaluator shall then specify a CKN and that the PSK is to be used as a CAK.</p> <p><b>TD0512 has been applied.</b></p>
<b>Test Steps</b>	<p><b>128-bit</b></p> <ul style="list-style-type: none"> <li>• Attempt to set a 128-bit key (32 hex digits). This will succeed.</li> <li>• Confirm keys in configuration.</li> <li>• Attempt to set a key of length 0. This will fail.</li> <li>• Attempt to set a key that is 31 hex digits in length. This will fail.</li> <li>• Attempt to set a key that is 33 hex digits in length. This will fail.</li> </ul> <p><b>256-bit</b></p> <ul style="list-style-type: none"> <li>• Attempt to set a 256-bit key (64 hex digits). This will succeed.</li> <li>• Confirm keys in configuration.</li> <li>• Attempt to set a key of length 0. This will fail.</li> <li>• Attempt to set a key that is 63 hex digits in length. This will fail.</li> <li>• Attempt to set a key that is 65 hex digits in length. This will fail.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to accept valid key lengths.</li> <li>• Evidence showing the storage of the valid keys.</li> </ul>

	<ul style="list-style-type: none"> <li>Evidence showing failure to store invalid key lengths</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE established a successful MACsec connection with good values and the TOE rejected bad values. This meets testing requirements.

### 6.141 FMT\_SMF.1/MACSEC Test #2

Item	Data
<b>Test Assurance Activity</b>	<p>The evaluator shall set up an environment where the TOE can connect to two other MACsec devices, identified as devices B and C, with the ability of pre-shared keys to be distributed between them. The evaluator shall configure the devices so that the TOE will be elected key server and principal actor, i.e., has highest key server priority.</p> <p>The evaluator will test the ability of the TOE to enable and disable MKA participants using the management function specified in the ST.</p> <p>The evaluator shall install pre-shared keys in devices B and C and take any necessary additional steps to create corresponding MKA participants. The evaluator shall disable the MKA participant on device C, then observe that the TOE can communicate with B but neither the TOE nor B can communicate with device C. The evaluator shall re-enable the MKA participant of device B and observe that the TOE is now able to communicate with devices B and C.</p> <p><b>TD0512 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>Initiate a MACsec connection with TOE from Peer B and Peer C.</li> <li>Confirm that Peer B can communicate with Peer C directly.</li> <li>Disable MACsec on Peer C.</li> <li>Verify that the TOE can communicate with Peer B but not with Peer C.</li> <li>Similarly, Peer B cannot communicate with Peer C.</li> <li>Re-enable MACsec back on for Peer C.</li> <li>Verify all the connections are good as before</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>The TOE should be able to connect with two MACsec peers B and C.</li> <li>Evidence (screenshot or CLI output) showing a successful connection of TOE with both the peers B and C.</li> <li>Packet capture showing a successful connection of TOE with both the peers B and C.</li> <li>Evidence (screenshot or CLI output) showing a successful connection of B with C.</li> <li>Packet capture showing a successful connection of B with C.</li> <li>Evidence (screenshot or CLI output) of disabling MACsec on peer C.</li> <li>Evidence (screenshot or CLI output) showing a connection failure of both TOE and peer B with peer C.</li> <li>Packet capture showing a connection failure of both TOE and peer B with peer C.</li> <li>Evidence (screenshot or CLI output) of enabling MACsec on peer C.</li> <li>Evidence (screenshot or CLI output) showing a successful connection of both TOE and peer B with peer C.</li> <li>Packet capture showing a successful connection of both TOE and peer B with peer C.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. When a non-TOE peer turns off the MACsec configuration, the TOE doesn't accept the traffic. Once the MACsec is enabled on the peer, secured channel was established between the TOE and peer. This meets testing requirement.

### 6.142 FMT\_SMF.1/MACSEC Test #3a

Item	Data
------	------

<b>Test Assurance Activity</b>	<p>Test 3: For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested. The tests are:</p> <p>Subtest a (Switch to unexpired CKN): TOE and Peer B have CKN1(10 minutes) and CKN2. CKN2 can either be configured with a longer overlapping lifetime (20 minutes) or be configured with a lifetime starting period of more than 10 minutes after the CKN1 start. The TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE expires SAK1. This can be verified by either 1) seeing the TOE immediately distribute a new SAK to the peer if the lifetime of CKN2 overlaps CKN1, or 2) by terminating the connection with CKN1 and distributing a new SAK once the lifetime period of CKN2 begins.</p> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Set on TOE a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 5678.</li> <li>• Set on Peer a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 5678.</li> <li>• Verify the start time and confirm that the session is using key 1234.</li> <li>• Verify that the session is using key 1234.</li> <li>• Verify via logs that the session is using key 1234 for 10 mins.</li> <li>• Verify via packet capture that the session is using key 1234.</li> <li>• Verify after 10 mins that the session uses key 5678.</li> <li>• Verify via logs after 10 mins that the session uses key 5678.</li> <li>• Verify via packet capture after 10 mins that the session uses key 5678.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Evidence (screenshot or CLI output) of configuring a lifetime of 10 minutes on key 1234 and a lifetime of 20 minutes on key 5678 on TOE and peer.</li> <li>• Logs showing the session is using key 1234 for 10 minutes.</li> <li>• Packet capture showing the session is using key 1234 for 10 minutes.</li> <li>• Logs showing the session is using key 5678 after 10 minutes.</li> <li>• Packet capture showing the session is using key 5678 after 10 minutes.</li> </ul>
<b>Pass/Fail with Explanation</b>	<p>Pass. The test performs re-keying at the configured time when the TOE is configured with a second key in the chain. The connection will delete the request from the peer and renegotiate with the new CAK. This meets the testing requirements.</p>

### 6.143 FMT\_SMF.1/MACSEC Test #3b

Item	Data
<b>Test Assurance Activity</b>	<p>Test 3: For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested. The tests are:</p> <p>Subtest b (reject CA with expired CKN): TOE has CKN1(10 minutes). Peer B has CKN1(20 minutes). TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE rejects (or ignores) peer's request to use (or distribute a) SAK using CKN1</p> <p><b>TD0652 has been applied.</b></p>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Set on TOE a lifetime of 10 minutes on key 1234.</li> <li>• Set on Peer a lifetime of 20 minutes only on key 1234.</li> <li>• Verify the start time and that the session is using key 1234.</li> <li>• Verify via packet capture that the session is using key 1234.</li> <li>• Verify via logs that the session is using key 1234 for 10 mins.</li> <li>• After the first CKN expires, the TOE rejects peers request to use SAK using CKN.</li> <li>• Verify the failure connection via packet capture.</li> <li>• Verify the failure connection via logs.</li> </ul>

<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• Logs showing the session is using key 1234 for 10 minutes.</li> <li>• Packet capture showing the session is using key 1234 for 10 minutes.</li> <li>• Logs showing the connection failure after 10 minutes</li> <li>• Packet capture showing the connection failure after 10 minutes</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE rejected peer request to distribute SAK using KKN. This meets the testing requirements.

#### 6.144 FMT\_SMF.1/MACSEC Test #4

Item	Data
<b>Test Assurance Activity</b>	If “Cause Key Server to generate a new group CAK...” is selected, the evaluator shall connect to the PAE of the TOE, set the management function specified in the ST (e.g., set ieee8021XKeyCreateNewGroup to true), and observe that the TOE distributes a new group CAK. <b>TD0512 has been applied.</b>
<b>Test Steps</b>	NA. The TOE does not support group CAKs.
<b>Expected Test Results</b>	NA. The TOE does not support group CAKs.
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not support group CAKs.

#### 6.145 FPT\_FLS.1(2)/SelfTest Test #1

Item	Data
<b>Test Assurance Activity</b>	The following test may require the vendor to provide access to a test platform that provides the evaluator with the ability to modify the TOE internals in a manner that is not provided to end customers: Test 1: The evaluator shall modify the TSF in a way that will cause a self-test failure to occur. The evaluator shall determine that the TSF shuts down and that the behavior of the TOE is consistent with the operational guidance. The evaluator shall repeat this test for each type of self-test that can be deliberately induced to fail. For TOEs with redundant failover capability, the evaluator shall determine that the failed components shut down and the behavior of the TOE is consistent with the operational guidance. For each component, the evaluator shall repeat each type of self-test that can be deliberately induced to fail. <b>TD0190 has been applied.</b>
<b>Test Steps</b>	<ul style="list-style-type: none"> <li>• Load the failure image and nist-test-cmds file onto the TOE.</li> <li>• Check the software authenticity and verify.</li> <li>• Assign the boot variable.</li> <li>• Reboot the device and observe the output.</li> <li>• Observe that during self-test, the boot fails.</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE shall reject modified boot images and fail to boot.</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE shuts down when a self-test failure occurs, and this behavior is consistent with the operational guidance. This meets the testing requirements.

### 6.146 FPT\_RPL.1 Test #1

Item	Data
<b>Test Assurance Activity</b>	Before performing each test the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction Test 1: The evaluator shall set up a MACsec connection with an entity in the Operational Environment. The evaluator shall then capture traffic sent from this remote entity to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the remote entity where the PN values in the SecTag of these packets are less than the lowest acceptable PN for the SA. The evaluator shall observe that the TSF does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.
<b>Test Steps</b>	Refer to the FCS_MACSEC_EXT.1 Test#1 test case for configuration. <ul style="list-style-type: none"> <li>• Use MACsec tool to replay MACsec traffic from peer.</li> <li>• Verify from packet capture that the reply to normal ping is received from TOE.</li> <li>• Verify from packet capture that repeated traffic is ignored. Note the PN values for the replay packets are same as normal ping</li> <li>• Verify that rejected traffic is logged</li> </ul>
<b>Expected Test Results</b>	<ul style="list-style-type: none"> <li>• The TOE should be able to establish successful MACsec traffic between TOE and peer device.</li> <li>• The TOE should not take action in response to the replayed traffic.</li> <li>• Evidence (screenshot or CLI output) of retransmitting copies of the traffic.</li> <li>• Packet capture of establishment of a MACsec session.</li> <li>• Evidence (screenshot or CLI output) of discarding the replayed traffic.</li> <li>• Packet capture of failure</li> </ul>
<b>Pass/Fail with Explanation</b>	Pass. The TOE does not respond to replayed packets. This meets the testing requirements.

### 6.147 FPT\_RPL.1 Test #2

Item	Data
<b>Test Assurance Activity</b>	Before performing each test the evaluator shall successfully establish a MACsec 27 channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction Test 2: The evaluator will capture frames during a MKA session and record the lowest PN observed in a particular time range. The evaluator will then send a frame with a lower PN, and then verify that this frame is dropped. The evaluator will verify that the device logged this event.
<b>Test Steps</b>	This test is covered by FPT_RPL.1 Test #1, where each duplicated encrypted ping has an invalid PN.
<b>Expected Test Results</b>	This test is covered by FPT_RPL.1 Test #1, where each duplicated encrypted ping has an invalid PN.
<b>Pass/Fail with Explanation</b>	Pass. This test is covered by FPT_RPL.1 Test #1, where each duplicated encrypted ping has an invalid PN.

### 6.148 FTP\_ITC.1/MACSEC Test #1

Item	Data
------	------

<b>Test Assurance Activity</b>	The evaluator shall evaluate this SFR in the manner specified in the NDcPP except that SNMPv3 and MACsec communications shall be tested in addition to any other selected protocols. Testing for these protocols is discussed in Section C.1.
<b>Pass/Fail with Explanation</b>	Pass. This test is covered throughout testing of MACsec and MKAs.

#### 6.149 FTP\_TRP.1/MACSEC Test #1

Item	Data
<b>Test Assurance Activity</b>	The evaluator shall evaluate this SFR in the manner specified in the NDcPP except that SNMPv3 communications shall be tested in addition to any selected protocols. Testing for SNMPv3 is discussed in Section C.1.
<b>Pass/Fail with Explanation</b>	Pass. This test is covered throughout testing of FCS_SSHS_EXT.1 and FCS_IPSEC_EXT.1.

## 7 Security Assurance Requirements

### 7.1 ADV\_FSP.1 Basic Functional Specification

#### 7.1.1 ADV\_FSP.1

##### 7.1.1.1 ADV\_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

##### 7.1.1.2 ADV\_FSP.1 Activity 2

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

##### 7.1.1.3 ADV\_FSP.1 Activity 3

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

### 7.2 AGD\_OPE.1 Operational User Guidance

#### 7.2.1 AGD\_OPE.1

##### 7.2.1.1 AGD\_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable
-----------	--



	guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on <a href="http://www.niap-ccevs.org">www.niap-ccevs.org</a> .  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 7.2.1.2 AGD\_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: <ul style="list-style-type: none"> <li>• Audit (syslog) Server</li> <li>• Local Console</li> <li>• Management Workstation with Secure Shell v2 (SSHv2) client</li> <li>• Remote Authentication Dial-In User Service (RADIUS) Authentication, Authorization, and Accounting (AAA) Server</li> <li>• Media Access Control security (MACsec) Peer</li> <li>• Certification Authority (CA)</li> <li>• TOE Peer</li> </ul> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 7.2.1.3 AGD\_OPE.1 Activity 3

Objective	The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.4 AGD\_OPE.1 Activity 4

Objective	The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.
Evaluator Findings	The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled <b>Excluded Functionality</b> specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.5 AGD\_OPE.1 Activity 5 [TD0536]

Objective	In addition, the evaluator shall ensure that the following requirements are also met.  <ul style="list-style-type: none"> <li>a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.</li> <li>b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps: <ul style="list-style-type: none"> <li>i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).</li> <li>ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature.</li> </ul> </li> <li>c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.</li> </ul>
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3.  The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2.  The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

**7.3 AGD\_PRE.1 Preparative Procedures**

7.3.1 AGD\_PRE.1

7.3.1.1 AGD\_PRE.1 Activity 1

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role
-----------	---

	to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).
Evaluator Findings	<p>The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the sections titled ‘Operational Guidance’ of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:</p> <ul style="list-style-type: none"> <li>• Audit (syslog) Server</li> <li>• Local Console</li> <li>• Management Workstation with Secure Shell v2 (SSHv2) client</li> <li>• Remote Authentication Dial-In User Service (RADIUS) Authentication, Authorization, and Accounting (AAA) Server</li> <li>• Media Access Control security (MACsec) Peer</li> <li>• Certification Authority (CA)</li> <li>• TOE Peer</li> </ul> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.3.1.2 AGD\_PRE.1 Activity 2

Objective	The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.									
Evaluator Findings	<p>The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including,</p> <ul style="list-style-type: none"> <li>• Cat8200 <ul style="list-style-type: none"> <li>○ C8200-1N-4T</li> <li>○ C8200L-1N-4T</li> <li>○ NIM: C-NIM-2T</li> </ul> </li> <li>• Cat8500 <ul style="list-style-type: none"> <li>○ C8500L-8S4X</li> </ul> </li> </ul> <p>The section titled Supported non-TOE Hardware/ Software/ Firmware of AGD identifies the following supported platform:</p> <p style="text-align: center;"><b>Table 1 IT Environment Components</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Component</th> <th style="text-align: center;">Required</th> <th style="text-align: center;">Usage/Purpose Description for TOE performance</th> </tr> </thead> <tbody> <tr> <td>RADIUS AAA Server</td> <td style="text-align: center;">Yes</td> <td>This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.</td> </tr> <tr> <td>Management Workstation with SSH Client</td> <td style="text-align: center;">Yes</td> <td>This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.</td> </tr> </tbody> </table>	Component	Required	Usage/Purpose Description for TOE performance	RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.	Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Component	Required	Usage/Purpose Description for TOE performance								
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.								
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.								

	Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
	Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
	MACSec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. It may be any device that supports MACsec communications.
	Remote VPN Gateway/Peer	Yes	This includes any VPN Peer (Gateway, Endpoint, another instance of the TOE) with which the TOE participates in VPN communications. Remote VPN Peers may be any device that supports IPsec VPN communications. Another instance of the TOE used as a VPN Peer would be installed in the evaluated configuration, and likely administered by the same personnel.
	Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

7.3.1.3 AGD\_PRE.1 Activity 3

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	<p>The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including,</p> <p>Insert list of functions, such as</p> <ul style="list-style-type: none"> <li>• <b>Configuring Administrative Accounts and Passwords</b> <ul style="list-style-type: none"> <li>○ Section 'Administrator Configuration and Credentials'</li> </ul> </li> <li>• <b>Configuring SSH and Console Connections</b> <ul style="list-style-type: none"> <li>○ Section 'Remote Administration Protocols'</li> </ul> </li> <li>• <b>Configuring the Remote Syslog Server</b> <ul style="list-style-type: none"> <li>○ Section 'Logging Protection'</li> </ul> </li> <li>• <b>Configuring Audit Log Options</b> <ul style="list-style-type: none"> <li>○ Section 'Logging Configuration'</li> </ul> </li> <li>• <b>Configuring Event Logging</b> <ul style="list-style-type: none"> <li>○ Section 'Usage of Embedded Event Manager'</li> </ul> </li> <li>• <b>Configuring a Secure Logging Channel</b> <ul style="list-style-type: none"> <li>○ Section 'Logging Protection'</li> </ul> </li> <li>• <b>Configuring VPNs (IPsec)</b> <ul style="list-style-type: none"> <li>○ Section 'Virtual Private Networks'</li> </ul> </li> <li>• <b>Configuring Traffic Filtering Rules</b> <ul style="list-style-type: none"> <li>○ Section 'Base Firewall Rule Set Configuration'</li> </ul> </li> <li>• <b>Configuring MACsec</b> <ul style="list-style-type: none"> <li>○ Section 'MACsec and MKA Configuration'</li> </ul> </li> </ul>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 7.3.1.4 AGD\_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

#### 7.3.1.5 AGD\_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met.  The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled ' <b>Remote Administration Protocols</b> and <b>Administrator Configuration and Credentials</b> ' were used to determine the verdict of this work unit. AGD describes entering enable secret, entering virtual terminal password, and enabling FIPS mode Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

## 7.4 ALC Assurance Activities

### 7.4.1 ALC\_CMC.1

#### 7.4.1.1 ALC\_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.  Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

7.4.2 ALC\_CMS.1

7.4.2.1 ALC\_CMS.1 Activity 1

Objective	When evaluating the developer’s coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

**7.5 ATE\_IND.1 Independent Testing – Conformance**

7.5.1 ATE\_IND.1

7.5.1.1 ATE\_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4.  The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.  Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

**7.6 AVA\_VAN.1 Vulnerability Survey**

7.6.1 AVA\_VAN.1

7.6.1.1 AVA\_VAN.1 Activity 1 [TD0564]

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.  Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator

searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- <https://nvd.nist.gov/vuln/search>
- <https://www.cisco.com/>
- <https://tools.cisco.com/security/center/softwarechecker.x>
- <http://nvd.nist.gov/>
- <http://www.securityfocus.com/>
- <https://www.cvedetails.com/>

The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on March 20,2023

Note that TD0564 states the following: “As the search terms can contain proprietary information and there is a possibility that this information could be used by attackers to identify potential attack surfaces, there is no expectation that search terms containing proprietary information are published in any public-facing document.” Due to the expanded search terms specified by Labgram #116, proprietary information may be present in the list of search terms and should be removed from the list provided below.

- TOE Name: C8200-1N-4T, C8200L-1N-4T, C8500L-8S4X
- Processors: Intel Xeon D-1563N (Broadwell) , Intel Xeon D-1573N (Broadwell), Intel Xeon D-2168NT (Skylake)  
MACsec: C-NIM-2T - Broadcom BCM54194, Broadcom BCM82757/BCM54194
- List of software and hardware components that compose the TOE.
  - Software components- IOS-XE 17.6, Syslog server, CA, VPN peer, Local console, MACsec peer
  - Independently identifiable and reusable components are not limited to those provided list. This list is required from vendors by Labgram -
- Crypto library

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 192 and 256)	IC2M	A1462	FCS_COP.1/DataEncryption FCS_COP.1(1)/KeyedHashCMAC FCS_COP.1(2)
		GCM (128, 192 and 256)			
		AES Key Wrap and CMAC (128, 256)			
		GCM (128, 256)	MACSec	4544 4550	
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	IC2M	A1462	FCS_COP.1/Hash

	HMAC (HMAC-SHA-1, SHA-256, SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	IC2M	A1462	FCS_COP.1/KeyedHash
	DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	IC2M	A1462	FCS_RBG_EXT.1
	RSA	Signature Verification and key transport	PKCS#1 v.1.5, 3072 bit key, FIPS 186-4 Key Gen	IC2M	A1462	FCS_CKM.1 FCS_COP.1/SigGen
	ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	IC2M	A1462	FCS_CKM.1 FCS_COP.1/SigGen
	CVL-KAS-ECC	Key Agreement	NIST Special Publication 800-56A	IC2M	A1462	FCS_CKM.2
	KAS-FFC-SSC	Key Agreement	NIST Special Publication 800-56A	IC2M	A1462	FCS_CKM.2
	<p>The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>					
Verdict	Pass					

#### 7.6.1.2 AVA\_VAN.1 Activity 2

Objective	<p>The evaluator shall perform the following activities to generate type 4 flaw hypotheses:</p> <ul style="list-style-type: none"> <li>• Fuzz testing <ul style="list-style-type: none"> <li>○ Examine effects of sending: <ul style="list-style-type: none"> <li>▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443)</li> <li>▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE.</li> </ul> </li> </ul> </li> </ul>
-----------	--



	<p>Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.</p> <ul style="list-style-type: none"> <li>○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well- formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.</li> </ul>
Evaluator Findings	<p>The evaluator documented the fuzz testing results with respect to this requirement.</p> <p>The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

### 7.6.1.3 AVA\_VAN.1/VPN Activity 1

Objective	<p>The evaluator shall perform the SAR Evaluation Activities defined in the NDcPP SD against the entire TOE (i.e., both the network device portion and the VPN gateway portion). In particular, the evaluator shall ensure that the vulnerability testing defined in section A.1.4 of the NDcPP SD is applied to the TOE's VPN interface(s) in addition to any other security-relevant network device interfaces that the TOE may have.</p>
Evaluator Findings	<p>The evaluation team performed a fuzzing test against the TOE to ensure only permitted, acceptable traffic would be able to pass through the interfaces protected by ACLs. The evaluation team documented this test and identified no issues with the product during execution of the test.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

## 8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

**End of Document**