Cisco Systems, Inc.

Cisco Web Security Appliance

Assurance Activity Report

Version 0.10

May 2022

Document prepared by

www.lightshipsec.com

Table of Contents

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security for the evaluation identified in Table 1. The AAR is produced in accordance with National Information Assurance Program (NIAP) reporting guidelines.

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Scheme	Canadian Common Criteria Scheme
Evaluation Facility	Lightship Security
Developer/Sponsor	Cisco Systems, Inc.
TOE	Cisco Web Security Appliance v11.8
Security Target	Cisco Web Security Appliance Security Target, v0.13
Protection Profile	collaborative Protection Profile for Network Devices, v2.2E (NDcPP), 23-March-2020

1.2 Evaluation Methods

2 The evaluation was performed using the methods, and standards identified in Table 2.

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1R5
Evaluation Methodology	CEM v3.1R5
Supporting Documents	Evaluation Activities for Network Device cPP, v2.2 (NDcPP-SD)
Interpretations	**NDcPP v2.2e** TD0527: Updates to Certificate Revocation Testing (FIA_X509_EXT.1) TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4 TD0536: NIT Technical Decision for Update Verification Inconsistency TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3 TD0538: NIT Technical Decision for Outdated link to allowed-with list

TD0546: NIT Technical Decision for DTLS - clarification of Application Note 63
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test
TD0556: NIT Technical Decision for RFC 5077 question
TD0563: NiT Technical Decision for Clarification of audit date information
TD0564: NiT Technical Decision for Vulnerability Analysis Search Criteria
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7
TD0570: NiT Technical Decision for Clarification about FIA_AFL.1
TD0571: NiT Technical Decision for Guidance on how to handle FIA_AFL.1
TD0572: NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors
TD0592: NIT Technical Decision for Local Storage of Audit Records

1.3 Reference Documents

Table 3: List of Reference Documents

Ref	Document
[ST]	Cisco Web Security Appliance Security Target, v0.13
[AGD]	Cisco Web Security Appliance running Async OS 11.8 Common Criteria Operational User Guidance And Preparative Procedures, v1.7
[ADMIN]	User Guide for AsyncOS 11.8 for Cisco Web Security Appliances – GD (General Deployment) First Published: 2020-04-22 Online version:

Ref	Document
	https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8.html
[ENT]	Cisco Web Security Appliance Entropy Information, Version 0.3

2 Evaluation Activities for SFRs

2.1 Security Audit (FAU)

2.1.1 FAU_GEN.1 Audit data generation

2.1.1.1 TSS

3 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.

Findings:	[ST] section 6.1 – FAU_GEN.1 – logs include reference to associated keys.

4 For distributed TOEs the evaluator shall examine the TSS to ensure that it describes which of the overall required auditable events defined in FAU_GEN.1.1 are generated and recorded by which TOE components. The evaluator shall ensure that this mapping of audit events to TOE components accounts for, and is consistent with, information provided in Table 1, as well as events in Tables 2, 4, and 5 (where applicable to the overall TOE). This includes that the evaluator shall confirm that all components defined as generating audit information for a particular SFR should also contribute to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component cover all the SFRs that it implements.

Findings:	The TOE is not a distributed TOE.

2.1.1.2 Guidance Documentation

5 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).

Findings:	[AGD] section 5 Table 8 lists the example audit events.

6 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.

Findings:	The evaluator made his determination of the administrative actions, by using FMT SFRs, FIA_PMG_EXT.1, FPT SFRs, and FTA SFRs, as a guide, and navigating through the user guide document for administrative actions related to those functional requirements, specifically, configuration changes related to TSF data and TSF. This includes the following sections in the [AGD]: Section 4.3 Password Complexity; Section 4.4 Adding a Login Banner;

Section 4.5.1 User Lockout;
Section 4.5.2 Inactive Session Termination;
Section 4.5.3 Session Termination;
Section 4.6 Setting the Time;
Section 4.7 Product Updates.

The evaluator also performed the administrative operations, involving changes to TSF data and TSF behaviour, as part of NDcPP v2.2E Test assurance activities, and confirmed that the documents provide sufficient information and instructions to enable evaluator to conduct NDcPP test requirements successfully.

2.1.1.3 Tests

7 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&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.

Findings: These tests are conducted throughout the test plan.

8 For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of auditable events to TOE components in the Security Target. For all events involving more than one TOE component when an audit event is triggered, the evaluator has to check that the event has been audited on both sides (e.g. failure of building up a secure communication channel between the two components). This is not limited to error cases but also includes events about successful actions like successful build up/tear down of a secure communication channel between TOE components.

Findings: The TOE is not a distributed TOE.

9 Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

2.1.2 FAU_GEN.2 User identity association

2.1.2.1 TSS

10 The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and Guidance Documentation requirements for FAU_GEN.1.

Findings: The requirements for FAU_GEN.1 are met. Therefore, this requirement also passes.

2.1.2.2 Guidance Documentation

11 The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and Guidance Documentation requirements for FAU_GEN.1.

Findings:	The requirements for FAU_GEN.1 are met. Therefore, this requirement also passes.

2.1.2.3 Tests

12 This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.

13 For distributed TOEs the evaluator shall verify that where auditable events are instigated by another component, the component that records the event associates the event with the identity of the instigator. The evaluator shall perform at least one test on one component where another component instigates an auditable event. The evaluator shall verify that the event is recorded by the component as expected and the event is associated with the instigating component. It is assumed that an event instigated by another component can at least be generated for building up a secure channel between two TOE components. If for some reason (could be e.g., TSS or Guidance Documentation) the evaluator would come to the conclusion that the overall TOE does not generate any events instigated by other components, then this requirement shall be omitted.

Findings:	The TOE is not a distributed TOE.

2.1.3 FAU_STG_EXT.1 Protected audit event storage

2.1.3.1 TSS

14 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.

Findings:	[ST] section 6.1 – FAU_STG_EXT.1 - indicates that the TOE can be configured to deliver logs to a remote server using SCP (SSH).

15 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.

Findings:	[ST] section 6.1 – FAU_STG_EXT.1 – the TSS states that the TOE can store a configurable number of logs up to a configurable size limit. If the space available for storing audit records is exhausted, the TOE will start to overwrite the oldest records. Only Authorized Administrators can clear the local logs, and there is no TOE interface that allows for administrators to modify the contents of the local audit records.

16 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.

Findings:	The TOE is not a distributed TOE.

17 The evaluator shall examine the TSS to ensure that it details the behaviour 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 behaviour of the TOE shall also be detailed in the TSS.

Findings:	As in the previous work units, section 6.1 of the [ST] states that if the space available for storing audit records is exhausted, the TOE will start to overwrite the oldest records.

18 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 real-time or periodically. In case the TOE does not perform transmission in real-time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible as well as acceptable frequency for the transfer of audit data.

Findings:	Section 6.1 of the [ST] under FAU_STG_EXT.1 indicates that the transmission is done based on configurable time and space rules provided by the administrator.

19 For distributed TOEs the evaluator shall examine the TSS to ensure it describes to which TOE components this SFR applies and how audit data transfer to the external audit server is implemented among the different TOE components (e.g. every TOE components does its own transfer or the data is sent to another TOE component for central transfer of all audit events to the external audit server).

Findings:	The TOE is not a distributed TOE.

20 For distributed TOEs the evaluator shall examine the TSS to ensure it describes which TOE components are storing audit information locally and which components are buffering audit information and forwarding the information to another TOE component for local storage. For every component the TSS shall describe the behaviour when local storage space or buffer space is exhausted.

Findings:	The TOE is not a distributed TOE.

2.1.3.2 Guidance Documentation

21 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.

Findings:	[AGD] section 3.4 provides protocol and version (SSHV2) and a pointer to the online user guide section "Pushing Log Files to Another Server". https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8/b_WSA_UserGuide_11_7_chapter_010101.html#task_1687223

	The link provides the steps to configure communication with the audit server.

22 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.

Findings:	[AGD] section 3.4 – logs a periodically archived via SCP according to an administrator defined time interval or log file size.

23 The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behaviour of the TOE for each possible configuration. The description of possible configuration options and resulting behaviour shall correspond to those described in the TSS.

Findings:	Section 3.4 of the [AGD] provides an appropriate level of information on the fact that admins can set both frequency- and log volume-based rules to push to the remote server. This is consistent with the information found in section 6.1 of the [ST] under FAU_STG_EXT.1.

2.1.3.3 Tests

24 Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement:

a) 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.

Note	Verification that the data is encrypted is satisfied by FTP_ITC.1 for the logging channel. The logging server uses SSHv2 described in the Test Setup. Due to the log-forwarding mechanism used on logging server, the audit records are therefore confirmed to have been successfully received by the audit server whenever the test cases are run.

b) 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 behaviour 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

1) The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after

the local storage for audit data is cleared (for the option ‘drop new audit data’ in FAU_STG_EXT.1.3).

2) The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option ‘overwrite previous audit records’ in FAU_STG_EXT.1.3)

3) The TOE behaves as specified (for the option ‘other action’ in FAU_STG_EXT.1.3).

High-Level Test Description
Configure a log subscription with a rollover capability. Show that the logs rollover when the configured thresholds are reached and overwrite the previous records.
Findings: PASS

c) Test 3: If the TOE complies with FAU_STG_EXT.2/LocSpace the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3

NOTE:	The ST does not claim this function.

d) Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.

NOTE:	The ST does not claim this function.

2.2 Cryptographic Support (FCS)

2.2.1 FCS_CKM.1 Cryptographic Key Generation

2.2.1.1 TSS

25 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.

Findings:	This information can be found in section 6.1 of the [ST] under FCS_CKM.1 and FCS_CKM.2. Specifically, the TOE is capable of generating 2048-bit (or greater) RSA keys for use in Remote Administration and for use in the SSH hostkey. The TOE also acts as a sender and receiver for Diffie-Hellman and EC Diffie-Hellman key establishment and therefore is responsible for key generation for those key establishment algorithms.

	The [ST] in section 6.1 for FCS_CKM.1 and FCS_CKM.2 provides a sub-table showing how each scheme is used. This sub-table is consistent with the claims and the testing.

2.2.1.2 Guidance Documentation

26 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.

Findings:	This information is provided in [AGD] section 3.2.1, which provides instructions for configuring FIPS mode and [AGD] section 3.3, which provides instructions for configuring network protocols and cryptographic settings. Operational key generation is configured for TLS. Section 3.3.4 of the [AGD] indicates that TLS RSA private keys can be generated via the "certconfig" CLI command. SSH hostkeys for the TOE are generated at software installation time and cannot be regenerated through standard operational means.

2.2.1.3 Tests

27 Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported).

Key Generation for FIPS PUB 186-4 RSA Schemes

28 The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent *e*, the private prime factors *p* and *q*, the public modulus *n* and the calculation of the private signature exponent *d*.

29 Key Pair generation specifies 5 ways (or methods) to generate the primes *p* and *q*. These include:

a. Random Primes:

- Provable primes
- Probable primes

b. Primes with Conditions:

- Primes p1, p2, q1,q2, p and q shall all be provable primes
- Primes p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes
- Primes p1, p2, q1,q2, p and q shall all be probable primes

30 To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.

Key Generation for Elliptic Curve Cryptography (ECC)

FIPS 186-4 ECC Key Generation Test

31 For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation.

FIPS 186-4 Public Key Verification (PKV) Test

32 For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values.

Key Generation for Finite-Field Cryptography (FFC)

33 The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y.

34 The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p:

- Primes q and p shall both be provable primes
- Primes q and field prime p shall both be probable primes

35 and two ways to generate the cryptographic group generator g:

- Generator g constructed through a verifiable process
- Generator g constructed through an unverifiable process.

36 The Key generation specifies 2 ways to generate the private key x:

- len(q) bit output of RBG where 1 <=x <= q-1
- len(q) + 64 bit output of RBG, followed by a mod q-1 operation and a +1 operation, where 1<= x<=q-1.

37 The security strength of the RBG must be at least that of the security offered by the FFC parameter set.

38 To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set.

39 For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm

- g != 0,1
- q divides p-1
- g^q mod p = 1
- g^x mod p = y

40 for each FFC parameter set and key pair.

[TD0580] FFC Schemes using "safe-prime" groups

41 Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.

Findings:	RSA key generation is covered by the following CAVP certificates all of which claim RSA KeyGen 186-4 for 2048-bit RSA keys: A397, A402, A403, A406,. These claims are consistent with FCS_CKM.1 in the [ST] section 5.2.2. ECDSA key generation is covered by the following CAVP certificates all of which claim ECDSA KeyGen 186-4 for NIST curves P-256, P-384 and P-521: A397, A402, A403, A406. These claims are consistent with FCS_CKM.1 in the [ST] section 5.2.2. FFC EC key generation is covered by the following CAVP certificates all of which claim KAS ECC Component for NIST curves P-256, P-384 and P-521: A397, A402, A403, A406. These claims are consistent with FCS_CKM.1 and FCS_CKM.2 in the [ST] section 5.2.2. Diffie-hellman group 14 is covered by additional testing below.

2.2.2 FCS_CKM.2 Cryptographic Key Establishment

2.2.2.1 [TD0580] TSS

42 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.

Findings:	[ST] section 6.1 – FCS_CKM.2 the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1.

43 The intent of this activity is to be able to identify the scheme being used by each service. This would mean, for example, one way to document scheme usage could be:

Scheme	SFR	Service
RSA	FCS_TLSS_EXT.1	Administration
ECDH	FCS_SSHC_EXT.1	Audit Server
ECDH	FCS_IPSEC_EXT.1	Authentication Server

44 The information provided in the example above does not necessarily have to be included as a table but can be presented in other ways as long as the necessary data is available.

Findings:	[ST] section 6.1 – FCS_CKM.2 provides a sub-table showing how each scheme is used.

2.2.2.2 Guidance Documentation

45 The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).

Findings:	This information is provided in [AGD] section 3.2.1, which provides instructions for configuring FIPS mode and [AGD] section 3.3, which provides instructions for configuring network protocols and cryptographic settings. Operational key establishment configuration is possible for both SSH and TLS. Section 3.3.2 of the [AGD] indicates that SSH key exchange algorithms can be configured using the "sshconfig" CLI command. Section 3.3.3 of the [AGD] provides the "sslconfig" CLI command to configure the TLS ciphers (which encode the key establishment algorithms as part of the ciphersuite specification).

2.2.2.3 [TD0580] Tests

Key Establishment Schemes

46 The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE using the applicable tests below.

SP800-56A Key Establishment Schemes

47 The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag.

Function Test

48 The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested.

49 The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and TOE id fields.

50 If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret.

51 The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.

52 If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm.

Validity Test

53 The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE id fields.

54 The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).

55 The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.

Findings:	FFC EC key generation is covered by the following CAVP certificates all of which claim KAS ECC Component for NIST curves P-256, P-384 and P-521: A397, A402, A403, A406. These claims are consistent with FCS_CKM.1 and FCS_CKM.2 in the [ST] section 5.2.2.

RSA-based key establishment schemes

56 The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 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 RSAES-PKCS1-v1_5.

High-Level Test Description
FCS_TLSS_EXT.1.3: Using a Lightship developed TLS client, connect to the TOE using a valid pure RSA ciphersuite and verify that the certificate that comes back from the Server Certificate message matches the expected bit size.
Findings: PASS

FFC Schemes using "safe-prime" groups

57 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.

High-Level Test Description
FCS_SSHS_EXT.1.7 Test 2: Using an independent SSH client, forcibly negotiate each of the claimed key exchange algorithms in turn and show that it results in a successful connection (the TOE claims group 14).
Findings: PASS

2.2.3 FCS_CKM.4 Cryptographic Key Destruction

2.2.3.1 TSS

58 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[1]). 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.

Findings:	Section 6.1 of the [ST] provides information on how keys and CSPs are zeroized. [ST] Annex A: Key Zeroization all keys are listed and zeroization method is described. The types of keys and CSPs are consistent with the claims made in section 5 of the [ST].

59 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).

Findings:	[ST] Annex A: Key Zeroization specifies that the key value is overwritten either by zeros or a new key value. As per the FCS_CKM.4 SFR in section 5 of the [ST], the TOE uses an abstraction to refer to the key.

60 Note that where selections involve '*destruction of reference*' (for volatile memory) or '*invocation of an interface'* (for non-volatile memory) then the relevant interface definition is examined by the evaluator to ensure that the interface supports the selection(s) and description in the TSS. In the case of non-volatile memory the evaluator includes in their examination the relevant interface description for each media type on which plaintext keys are stored. The presence of OS-level and storage device-level swap and cache files is not examined in the current version of the Evaluation Activity.

Findings:	The ST does not claim "destruction of reference" or "invocation of an interface".

61 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

[1] Where keys are stored encrypted or wrapped under another key then this may need to be explained in order to allow the evaluator to confirm the consistency of the description of keys with the TOE functions.

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.

Findings:	Section 7 of the [ST] lists a 256 AES Encryption Key which is used to encrypt passwords, authentication information, certificates, and shared keys.

62 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.

Findings:	The [ST] TSS identifies no configurations or circumstances that may not conform to the key destruction requirement.

63 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.

Findings:	N/A - The use of "a value that does not contain any CSP" is not included in the ST.

2.2.3.2 Guidance Documentation

64 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.

65 For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-levelling and garbage collection. This may result in additional copies of the key that are logically inaccessible but persist physically. Where available, the TOE might then describe use of the TRIM command[2] and garbage collection to destroy these persistent copies upon their deletion (this would be explained in TSS and Operational Guidance).

Findings:	Section 3.3.7.1 of the [AGD] provides information where key material might be present in coredump files which are often generated as a result of error conditions. Such coredump files can be overwritten with zeros using the "wipedata" CLI command.

2.2.3.3 Tests

66 None

[2] Where TRIM is used then the TSS and/or guidance documentation is also expected to describe how the keys are stored such that they are not inaccessible to TRIM, (e.g. they would need not to be contained in a file less than 982 bytes which would be completely contained in the master file table).

2.2.4 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

2.2.4.1 TSS

67 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.

Findings:	[ST] section 6.1 – FCS_COP.1/DataEncryption The TOE provides symmetric encryption and decryption capabilities using AES in CBC, CTR, and GCM mode (128 and 256 bits).

2.2.4.2 Guidance Documentation

68 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.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement and [AGD] section 3.3, which provides instructions for configuring network protocols and cryptographic settings.

2.2.4.3 Tests

AES-CBC Known Answer Tests

69 There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

70 **KAT-1.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.

71 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.

72 **KAT-2.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

73 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.

74 **KAT-3.** To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key *i* in each set shall have the leftmost *i* bits be ones and the rightmost *N-i* bits be zeros, for *i* in [1,N].

75 To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

76 **KAT-4.** To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].

77 To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test

78 The evaluator shall test the encrypt functionality by encrypting an *i*-block message where 1 < *i* <=10. The evaluator shall choose a key, an IV and plaintext message of length *i* blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

79 The evaluator shall also test the decrypt functionality for each mode by decrypting an *i*-block message where 1 < *i* <=10. The evaluator shall choose a key, an IV and a ciphertext message of length *i* blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CBC Monte Carlo Tests

80 The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

```
# Input: PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
```

```
        PT = IV
    else:
        CT[i] = AES-CBC-Encrypt(Key, PT)
        PT = CT[i-1]
```

81 The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

82 The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

AES-GCM Test

83 The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

128 bit and 256 bit keys

a. **Two plaintext lengths**. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.

a. **Three AAD lengths**. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.

b. **Two IV lengths**. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

84 The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

85 The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

86 The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

AES-CTR Known Answer Tests

87 The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. Since the Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. The generation and management of the counter is tested through FCS_SSH*_EXT.1.4. If CBC and/or GCM are selected in FCS_COP.1/DataEncryption, the test activities for those modes sufficiently demonstrate the correctness of the AES algorithm. If CTR is the only selection in FCS_COP.1/DataEncryption, the AES-CBC Known Answer Test, AES-GCM Known Answer Test, or the following test shall be performed (all of these tests demonstrate the correctness of the AES algorithm):

88 There are four Known Answer Tests (KATs) described below to test a basic AES encryption operation (AES-ECB mode). For all KATs, the plaintext, ~~IV,~~ and ciphertext values shall be 128-bit blocks. The results from each test may the validator obtain either directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

89 KAT-1 To test the encrypt functionality, the evaluator shall supply a set of 5 plaintext values for each selected keysize and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros.

90 KAT-2 To test the encrypt functionality, the evaluator shall supply a set of 5 key values for each selected keysize and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value.

91 KAT-3 To test the encrypt functionality, the evaluator shall supply a set of key values for each selected keysize as described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values. A set of 128 128-bit keys, a set of 192 192-bit keys, and/or a set of 256 256-bit keys. Key_i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1, N].

92 KAT-4 To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the ciphertext values that result from encryption of the given plaintext using each selected keysize with a key value of all zeros (e.g. 256 ciphertext values will be generated if 128 bits and 256 bits are selected and 384 ciphertext values will be generated if all keysizes are selected). Plaintext value i in each set shall have the leftmost bits be ones and the rightmost 128-i bits be zeros, for i in [1, 128].

AES-CTR Multi-Block Message Test

93 The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 less-than i less-than-or-equal to 10 (test shall be performed using AES-ECB mode). For each i the evaluator shall choose a key and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key using a known good implementation. The evaluator shall perform this test using each selected keysize.

AES-CTR Monte-Carlo Test

94 The evaluator shall test the encrypt functionality using 100 plaintext/key pairs. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows:

```
# Input: PT, Key
for i = 1 to 1000:
CT[i] = AES-ECB-Encrypt(Key, PT) PT = CT[i]
```

95 The ciphertext computed in the 1000th iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall perform this test using each selected keysize.

96 There is no need to test the decryption encryption.

Findings:	AES encryption and decryption is covered by the following CAVP certificates all of which claim AES with key sizes of 128- and 256-bits: A397, A402, A403, A406. These claims are consistent with FCS_COP.1/DataEncryption in the [ST] section 5.2.2.

2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification

2.2.5.1 TSS

97 The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.

Findings:	[ST] section 6.1 – FCS_COP.1/SigGen The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048.

2.2.5.2 Guidance Documentation

98 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.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement and [AGD] section 3.3, which provides instructions for configuring network protocols and cryptographic settings.

2.2.5.3 Tests

ECDSA Algorithm Tests

ECDSA FIPS 186-4 Signature Generation Test

99 For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator shall use the signature verification function of a known good implementation.

ECDSA FIPS 186-4 Signature Verification Test

100 For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.

RSA Signature Algorithm Tests

Signature Generation Test

101 The evaluator generates or obtains 10 messages for each modulus size/SHA combination supported by the TOE. The TOE generates and returns the corresponding signatures.

102 The evaluator shall verify the correctness of the TOE's signature using a trusted reference implementation of the signature verification algorithm and the associated public keys to verify the signatures.

Signature Verification Test

103 For each modulus size/hash algorithm selected, the evaluator generates a modulus and three associated key pairs, (*d*, *e*). Each private key *d* is used to sign six pseudorandom messages each of 1024 bits using a trusted reference implementation of the signature generation algorithm. Some of the public keys, *e*, messages, or signatures are altered so that signature verification should fail. For both the set of original messages and the set of altered messages: the modulus, hash algorithm, public key *e* values, messages, and signatures are forwarded to the TOE, which then attempts to verify the signatures and returns the verification results.

104 The evaluator verifies that the TOE confirms correct signatures on the original messages and detects the errors introduced in the altered messages.

Findings:	The ST does not claim ECDSA signature generation or verification. RSA Signature Generation and Verification is covered by the following CAVP certificates all of which claim RSA SigGen 186-4 using PKCS 1.5 and 2048-bit RSA keys as well as RSA SigVer 186-4 using PKCS 1.5 and 2048-bit RSA keys: A397, A402, A403, A406. These claims are consistent with FCS_COP.1/SigGen in the [ST] section 5.2.2.

2.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

2.2.6.1 TSS

105 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.

Findings:	[ST] section 6.1 – FCS_COP.1/Hash describes the use of the hash functions within the TOE.

2.2.6.2 Guidance Documentation

106 The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.

Findings:	Section 3.3.2 of the [AGD] provides an administrator a means to configure the HMAC for TOE server-side SSH protocol using the "sshconfig" CLI command. Section 3.3.3 of the [AGD] permits the administrator to configure the set of TLS ciphersuites that can be used by the TOE for the web interface using the "sslconfig" CLI command. In both cases, the [AGD] provides the set of permitted values that meet the evaluated configuration. The [AGD] indicates in section 3.2.1 that it is necessary to operate the device in FIPS mode to automatically configure the FIPS approved algorithms and key sizes.

2.2.6.3 Tests

107 The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the

TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs.

108 The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

Short Messages Test - Bit-oriented Mode

109 The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Short Messages Test - Byte-oriented Mode

110 The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Bit-oriented Mode

111 The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the ith message is m + 99*i, where 1 ≤ i ≤ m. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test - Byte-oriented Mode

112 The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the ith message is m + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Test

113 This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

Findings:	Hashing is covered by the following CAVP certificates all of which claim SHA1 and SHA2-256, SHA2-384 and SHA2-512: A397, A402, A403, A406. These claims are consistent with FCS_COP.1/Hash in the [ST] section 5.2.2.6 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm).

2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

2.2.7.1 TSS

114 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.

Findings:	[ST] section 6.1 – FCS_COP.1/KeyedHash specifies the TOE provides keyed-hashing message authentication services using HMAC-SHA-1, key size 160 bits, and message digest sizes 160 bits as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. The block size for HMAC-SHA1 is 512 bits.

2.2.7.2 Guidance Documentation

115 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.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement.

2.2.7.3 Tests

116 For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and message data using a known good implementation.

Findings:	HMAC is covered by the following CAVP certificates all of which claims HMAC-SHA1: A397, A402, A403, A406. These claims are consistent with FCS_COP.1/KeyedHash in the [ST] section 5.2.2.

2.2.8 FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

117 Documentation shall be produced—and the evaluator shall perform the activities—in accordance with Appendix D of [NDcPP].

2.2.8.1 TSS

118 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.

Findings:	According to section 6.1 of the [ST] under FCS_RBG_EXT.1, “The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90 seeded by an entropy source that accumulates entropy from a TSF-software based noise source as described in FCS_RBG_EXT.1. This output is used directly to seed the DRBG.” Furthermore, the “deterministic RBG is seeded with a minimum of 256 bits of entropy.”

2.2.8.2 Guidance Documentation

119 The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement.

2.2.8.3 Tests

120 The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration.

121 If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. “generate one block of random bits” means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

122 If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

123 The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

Entropy input: the length of the entropy input value must equal the seed length.

Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.

Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

Findings:	AES CTR-mode DRBG is covered by the following CAVP certificates which all claim use of a 256-bit key: A397, A402, A403, A406. These claims are consistent with FCS_RBG_EXT.1 in the [ST] section 5.2.2.

2.3 Identification and Authentication (FIA)

2.3.1 FIA_AFL.1 Authentication Failure Management

2.3.1.1 TSS

124 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.

Findings:	[ST] section 6.1 – FIA_AFL.1 specifies that when the Authorized Administrator attempting to log into the administrative CLI or GUI interface 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 an Authorized Administrator resets the user's number of failed login attempts through the administrative CLI.

125 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).

Findings:	[ST] section 6.1 – FIA_AFL.1 specifies the “admin” default user account that has full access to all system configuration settings. Note, this account is not subject to the lock out at the local console.

2.3.1.2 Guidance Documentation

126 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.

Findings:	[AGD] section 4.5.1 provides information to the administrator to configure the lockout parameters and to unlock the users. The only action available to the administrator is to manually unlock users. Unlocking users can be done using the CLI (“userconfig”) or the GUI.

127 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.

Findings:	[AGD] section 4.1 - informs administrators that the “admin” user is not susceptible to lockout at the local console and can be used to rescue the system if necessary.

2.3.1.3 Tests

128 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):

a. 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.

High-Level Test Description
Configure the account locking mechanism to 5 attempts. Lock out the user with 5 bad attempts and show that the 6th is denied even if the proper password is used. Using the administrator account, unlock the locked user and then show that the user can log in again. Repeat the above for both SSH and Web UI interfaces. Show that users cannot be locked out at the local console.
Findings: PASS

b. Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows.

If the administrator action 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).

If the time period selection in FIA_AFL.1.2 is included in the ST then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorisation attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.

Note:	See previous test case. The [ST] only claims the use of an administrative unlock.

2.3.2 FIA_PMG_EXT.1 Password Management

2.3.2.1 TSS

129 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.

Findings:	[ST] section 6.1 – FIA_PMG_EXT.1 includes a list of special characters and specifies the minimum (0) and maximum (128) number of characters supported for administrator passwords. The [ST] further specifies that in the evaluated configuration the minimum password length is set to at least 15.

2.3.2.2 Guidance Documentation

130 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.

Findings:	[AGD] 4.3 identifies the supported characters and provides guidance on strong passwords. Section Perform System Administration Tasks – Configuring Restrictive User Account and Passphrase Settings of the online user guide specifies “You can define how many failed login attempts cause the user to be locked out of the account. You can set the number of user login attempts from 1 to 60. The default value is 5.”

2.3.2.3 Tests

131 The evaluator shall perform the following tests.

a. Test 1: 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.

High-Level Test Description
Change the minimum required password length to be 15 characters using supported characters. Change the password for the built-in ‘admin’ user using the identified TSFI. Show that the password can be used to login to the Web GUI, SSH and local console.
Findings: PASS

b. Test 2: 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.

High-Level Test Description
Change the minimum required password length to be 8 characters. Change the password for the built-in ‘admin’ back to a known good password. Using the admin account, change the password for another user to be only 7 characters and show it is rejected. Change the password for another user to be 8 characters and show it is accepted. Repeat this on the CLI and Web UI.
Findings: PASS

2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

2.3.3.1 TSS

132 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".

Findings:	[ST] section 6.1 – FIA_UIA_EXT.1 "The TOE provides a local password-based authentication mechanism for the CLI when accessed both locally and remotely as well as the GUI. When the CLI is accessed remotely, the session is secured via SSHv2 and authenticated using SSH public key." The [ST] has the necessary information about how the TOE processes the logging in operation.

133 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.

Findings:	[ST] section 6.1 – FIA_UIA_EXT.1 "The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed, except for the login banner that is displayed prior to user authentication." This is consistent with the claims made in section 5.2 of the [ST].

134 For distributed TOEs the evaluator shall examine that the TSS details how Security Administrators are authenticated and identified by all TOE components. If not all TOE components support authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the TSS shall describe how the overall TOE functionality is split between TOE components including how it is ensured that no unauthorized access to any TOE component can occur.

Findings:	The TOE is not a distributed TOE.

135 For distributed TOEs, the evaluator shall examine the TSS to determine that it describes for each TOE component which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. For each TOE component that does not support authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2 the TSS shall describe any unauthenticated services/services that are supported by the component.

Findings:	The TOE is not a distributed TOE.

2.3.3.2 Guidance Documentation

136 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.

Findings:	[AGD] section 3.3.2 provides guidance on SSHv2 configuration, which includes preparatory steps. [AGD] section 3.3.6 provides guidance for enabling a certificate for the HTTPS interface. Information about how to log onto the TOE over the remote SSH CLI and local serial port can be found in [ADMIN] in section “Accessing the Command Line Interface”. Logging onto the device using the remote Web UI interface is provided in [ADMIN] in section “Accessing the Appliance Web Interface.” The evaluator has verified that the guidance documents include the necessary preparatory steps.

2.3.3.3 Tests

137 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:

a. 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&A information results in the ability to access the system, while providing incorrect information results in denial of access.

High-Level Test Description
Log into the identified management interface using a known-good credential and logout. Attempt to log into the management interface using a known-bad credential and verify the TOE denies access. Ensure the appropriate audit messages appear.
Findings: PASS

b. 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.

High-Level Test Description
The device does not have any services configured prior to I&A. All claimed services available to remote entities are identified as part of AVA_VAN.1 test scanning.
Findings: PASS

c. 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.

High-Level Test Description
The device does not have any services configured prior to I&A.

High-Level Test Description
All claimed services available to local entities are identified as part of AVA_VAN.1 test scanning.
Findings: PASS

d. Test 4: For distributed TOEs where not all TOE components support the authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the evaluator shall test that the components authenticate Security Administrators as described in the TSS.

Note: The TOE is not a distributed TOE.

2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

138 Evaluation Activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1.

2.3.5 FIA_UAU.7 Protected Authentication Feedback

2.3.5.1 TSS

139 None.

2.3.5.2 Guidance Documentation

140 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.

Findings:	The default configuration of the TOE does not reveal authentication data at any login prompt.

2.3.5.3 Tests

141 The evaluator shall perform the following test for each method of local login allowed:

a. Test 1: 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.

High-Level Test Description
Log into the local management interface. Ensure the password field does not echo characters – even a masking character -- as claimed by the ST.
Findings: PASS

2.4 Security management (FMT)

2.4.1 General requirements for distributed TOEs

2.4.1.1 TSS

142 For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.

Findings:	The TOE is not a distributed TOE.

2.4.1.2 Guidance Documentation

143 For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.

Findings:	The TOE is not a distributed TOE.

2.4.1.3 Tests

144 Tests defined to verify the correct implementation of security management functions shall be performed for every TOE component. For security management functions that are implemented centrally, sampling should be applied when defining the evaluator's tests (ensuring that all components are covered by the sample).

Findings:	The TOE is not a distributed TOE.

2.4.2 FMT_MOF.1/ManualUpdate Management of security functions behaviour

2.4.2.1 TSS

145 For distributed TOEs see chapter 2.4.1.1. There are no specific requirements for non-distributed TOEs.

Findings:	The TOE is not a distributed TOE.

2.4.2.2 Guidance Documentation

146 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).

Findings:	[AGD] section 2 outlines the method for performing a manual update.

147 For distributed TOEs the guidance documentation shall describe all steps how to update all TOE components. This shall contain description of the order in which components need to be updated if the order is relevant to the update process. The guidance documentation shall also provide warnings regarding functions of TOE

components and the overall TOE that may cease to operate during the update (if applicable).

Findings:	The TOE is not a distributed TOE.

2.4.2.3 Tests

148 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.

149 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.

High-Level Test Description
Log into the Web GUI using an account with privileges which should not permit upgrades. Attempt to upgrade the device. The action should fail. Log into the CLI using an account with privileges which should not permit upgrades. Attempt to upgrade the device. The action should fail.
Findings: PASS

2.4.3 FMT_MTD.1/CoreData Management of TSF Data

2.4.3.1 TSS

150 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.

Findings:	[ST] section 6.1 – FMT_MTD.1 "No administrative functionality is available prior to the Authorized Administrators logging in." This is consistent with the selections made in section 5.2.

151 If 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.

Findings:	[ST] section 6.1 – FMT_MTD.1 "The TOE also provides the ability for Authorized Administrators to generate and manage the cryptographic keys that used to secure connections on the TOE. The Authorized Administrators accesses the CLI for management of the cryptographic functions."

2.4.3.2 Guidance Documentation

152 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.

Findings:	Guidance for all TSF-data-manipulating functions have been reviewed as shown in the Guidance Documentation requirements for all other SFRs in this AAR. [AGD] section 4.1 provides guidance for role based access control.

153 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.

Findings:	[AGD] section 3.3.4 provides guidance on obtaining X.509 certificates and generating CSRs. [AGD] section 3.3.5 provides guidance for installing certificates in the trust store. [AGD] 3.3.6 provides guidance on specifying the certificate to be used for HTTPS. The [AGD] also includes a reference to the following website which provides trust anchor guidance in [ADMIN] the section titled "Managing Trusted Root Certificates". https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8/b_WSA_UserGuide_11_7_chapter_010110.html?bookSearch=true#task_1431848

2.4.3.3 Tests

154 No separate testing for FMT_MTD.1/CoreData is required unless one of the management functions has not already been exercised under any other SFR.

2.4.4 FMT_SMF.1 Specification of Management Functions

155 The security management functions for FMT_SMF.1 are distributed throughout the cPP and are included as part of the requirements in FTA_SSL_EXT.1, FTA_SSL.3, FTA_TAB.1, FMT_MOF.1/ManualUpdate, FMT_MOF.1/AutoUpdate (if included in the ST), FIA_AFL.1, FIA_X509_EXT.2.2 (if included in the ST), FPT_TUD_EXT.1.2 & FPT_TUD_EXT.2.2 (if included in the ST and if they include an administrator-configurable action), FMT_MOF.1/Services, and FMT_MOF.1/Functions (for all of these SFRs that are included in the ST), FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.

2.4.4.1 TSS (containing also requirements on Guidance Documentation and Tests)

156 The evaluator shall examine the TSS, Guidance Documentation and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT_SMF.1 are provided by the TOE. The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).

Findings:	[ST] section 6.1 – FMT_SMF.1 "The CLI is the main interface used to administer the TOE since all functionality to configure, securely manage and to monitor the TOE is available via the CLI. The GUI interface can also be used however not all functionality to configure the TOE is available in the GUI. Therefore, in the evaluated configuration it is recommended to use the CLI."

	In the [ST] in section 5.2, the set of functions available to manage the TOE are listed. For each function, we found a corresponding description of the function described in the set of guidance documents. a) Ability to administer the TOE locally and remotely: this is performed over the local and remote interfaces as described in [AGD] in section 3.2 and supported by additional information from [ADMIN] (see information provided in work units for FIA_UIA_EXT.1). b) Ability to configure the access banner: The CLI and web access banners are configured as per section 4.4 of the [AGD]. c) Ability to configure the session inactivity time before session termination or locking: Session inactivity termination settings for both Web UI and CLI (local and remote) are configured as per section 4.5.2 of [AGD]. d) Ability to update the TOE and to verify the updates: TOE upgrades and verification is performed according to the instructions provided in section 2 of the [AGD]. More information can be found in work units for FMT_MOF.1/ManualUpdate. e) Ability to configure the authentication failure parameters: Authentication failure handling is described in [AGD] section 4.5.1. More information can be found in work units for FIA_AFL.1. f) Ability to configure audit behaviour: Information about modifying the remote logging parameters is provided in [AGD] section 3.4. g) Ability to configure the cryptographic functionality: Cryptographic parameters for both SSH and TLS can be configured. SSH parameters are described in section 3.3.2 of [AGD] and TLS parameters are described in section 3.3.3 of [AGD]. h) Ability to manage the cryptographic keys: The TOE can generate private keys for its own use with the web interface X.509 certificate. Instructions for generating this key is found in section 3.3.4 of [AGD]. i) Ability to re-enable an Administrator account: This function is described in section 4.5.1 of [AGD]. Additional information can be found in work units for FIA_AFL.1. j) Ability to set the time which is used for timestamps: Being able to set the date/time is described in section 4.6 of [AGD]. k) Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors: This information is provided in [AGD] section 3.3.5. Additional information is provided in work units for FMT_MTD.1/CoreData. l) Ability to import X.509v3 certificates to the TOE's trust store: This information is provided in [AGD] section 3.3.5. Additional information is provided in work units for FMT_MTD.1/CoreData.

157 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.

Findings:	[ST] section 6.1 – FMT_SMF.1 The local interface is described. [AGD] section 1.5 defines the local connection as “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.”

158 For distributed TOEs with the option 'ability to configure the interaction between TOE components' the evaluator shall examine that the ways to configure the interaction between TOE components is detailed in the TSS and Guidance Documentation. The evaluator shall check that the TOE behaviour observed during testing of the configured SFRs is as described in the TSS and Guidance Documentation.

Findings:	The TOE is not a distributed TOE.

2.4.4.2 Guidance Documentation

159 See section 2.4.4.1.

2.4.4.3 Tests

160 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.

2.4.5 FMT_SMR.2 Restrictions on security roles

2.4.5.1 TSS

161 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.

Findings:	[ST] section 6.1 – FMT_SMR.2 “The TOE maintains Authorized Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely.”

2.4.5.2 Guidance Documentation

162 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.

Findings:	**I**nformation about how to log onto the TOE over the remote SSH CLI and local serial interface can be found in [ADMIN] in section “Accessing the Command Line Interface”. Logging onto the device using the remote Web UI interface is provided in [ADMIN] in section “Accessing the Appliance Web Interface.”

2.4.5.3 Tests

163 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.

Findings:	All interfaces are tested as described in the guidance documentation.

2.5 Protection of the TSF (FPT)

2.5.1 FPT_APW_EXT.1 Protection of Administrator Passwords

2.5.1.1 TSS

164 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.

Findings:	[ST] section 6.1 – FPT_APW_EXT.1 specifies that passwords are stored encrypted. This section also specifies "The encrypted passwords and keys are stored in their respective configuration files and there are no administrative interfaces available to access the data." Additionally, Annex A of the [ST] includes an AES 256-bit key which is used to encrypt passwords.

2.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)

2.5.2.1 TSS

165 The evaluator shall examine the TSS to determine that it 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, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Findings:	[ST] Annex A: Key Zeroization lists all keys and the storage method. [ST] section 6.1 – FPT_SKP_EXT.1 "The encrypted passwords and keys are stored in their respective configuration files and there are no administrative interfaces available to access the data."

2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

2.5.3.1 TSS

166 The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

Findings:	[ST] section 6.1 – FPT_STM_EXT.1 specifies the following information: "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 setting the system time and administrative session timeout." The evaluator has verified that the [ST] includes the required information.

2.5.3.2 Guidance Documentation

167 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.

Findings:	[AGD] section 4.6 addresses how to manually set the time by the administrator. The ST does not claim use of an NTP server.

2.5.3.3 Tests

168 The evaluator shall perform the following tests:

a. Test 1: If the TOE supports direct setting of the time by the Security Administrator 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.

High-Level Test Description
Using the CLI as a privileged admin, show the current date/time and then change the current date time. Show the changed date/time is accepted. Using the Web UI as a privileged admin, show the current date/time and then change the current date time. Show the changed date/time is accepted.
Findings: PASS

a. Test 2: If the TOE supports the use of an NTP server; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.

Test Not Applicable:	The ST does not claim NTP.

169 If the audit component of the TOE consists of several parts with independent time information, then the evaluator shall verify that the time information between the different parts is either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.

Findings:	The TOE does not support independent time information.

2.5.4 FPT_TST_EXT.1 TSF testing

2.5.4.1 TSS

170 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.

Findings:	[ST] section 6.1 – FPT_TST_EXT.1 lists the self-tests that are run by the TOE and provides the following argument “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 behaviour will be identified by the failure of a self-test.” The evaluator has verified that the [ST] has the required information and the argument is sufficient to ensure the TSF is operating correctly.

171 For distributed TOEs the evaluator shall examine the TSS to ensure that it details which TOE component performs which self-tests and when these self-tests are run.

Findings:	The TOE is not a distributed TOE.

2.5.4.2 Guidance Documentation

172 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.

Findings:	[AGD] section 7 offers a summary of the modes of operation of the TOE. Specific errors related to power-on self-tests are described in section 3.3.7 of [AGD] as well as the steps needed to respond to such errors.

173 For distributed TOEs the evaluator shall ensure that the guidance documentation describes how to determine from an error message returned which TOE component has failed the self-test.

Findings:	The TOE is not a distributed TOE.

2.5.4.3 Tests

174 It is expected that at least the following tests are performed:

a. Verification of the integrity of the firmware and executable software of the TOE

b. Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.

175 Although formal compliance is not mandated, the self-tests performed should aim for a level of confidence comparable to:

a. [FIPS 140-2], chap. 4.9.1, Software/firmware integrity test for the verification of the integrity of the firmware and executable software. Note that the testing is not restricted to the cryptographic functions of the TOE.

b. [FIPS 140-2], chap. 4.9.1, Cryptographic algorithm test for the verification of the correct operation of cryptographic functions. Alternatively, national requirements of any CCRA member state for the security evaluation of cryptographic functions should be considered as appropriate.

176 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.

High-Level Test Description
The evaluator reviewed the CMVP certificate for the Cisco FOM version 6.2 which is used in the TOE. The FIPS 140-2 Security Policy includes cryptographic algorithm tests for all claimed algorithms. https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2984.pdf The developer aided testing of the secure boot functionality which includes an integrity test. The developer modified the TOE; this made the integrity test to fail which caused the TOE to enter an error state.
Findings: PASS

177 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.

Note: The TOE is not a distributed TOE.

2.5.5 FPT_TUD_EXT.1 Trusted Update

2.5.5.1 TSS

178 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.

Findings:	[ST] section 6.1 – FPT_TUD_EXT.1 describes that both the CLI and GUI can be used to query the currently active version of the TOE software/firmware. The TOE does not support delayed activation.

179 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.

Findings:	[ST] section 6.1 – FPT_TUD_EXT.1 describes that the TOE uses a published SHA2-512 hash to validate the TOE firmware. The administrator is required to manually verify the hash before confirming that the new image can be installed

180 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.

Findings:	Section 5.2 of the [ST] has not selected this option for FPT_TUD_EXT.1.2.

181 For distributed TOEs, the evaluator shall examine the TSS to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. Alternatively, this description can be provided in the guidance documentation. In that case the evaluator should examine the guidance documentation instead.

Findings:	The TOE is not a distributed TOE.

182 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.

Findings:	Section 6.1 of the [ST] in section FPT_TUD_EXT.1 indicates that an administrator is required to actively confirm manual installation of the new image after an independent check has been conducted.

2.5.5.2 Guidance Documentation

183 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.

Findings:	[AGD] section 2 identifies the ‘version’ CLI command to query the current version of the TOE. Delayed activation is not supported.

184 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.

Findings:	[AGD] section 2 identifies the steps to verify the published hash. When performing an update using the online Cisco update servers, the procedure to validate the hash requires a bit more involvement from the administrator.

185 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.

Findings:	[AGD] section 2 identifies the steps to obtain the published hash. The authentic hash is provided by the Cisco update servers in the manifest file. This information can be viewed in the upgrade_logs and updater_logs. This information is retrieved over HTTPS from the Cisco upgrade servers.

186 For distributed TOEs the evaluator shall verify that the guidance documentation describes how the versions of individual TOE components are determined for FPT_TUD_EXT.1, how all TOE components are updated, and the error conditions that may arise from checking or applying the update (e.g., failure of signature verification, or exceeding available storage space) along with appropriate recovery actions. The guidance documentation only has to describe the procedures relevant

for the user; it does not need to give information about the internal communication that takes place when applying updates.

Findings:	The TOE is not a distributed TOE.

187 If this was information was not provided in the TSS: For distributed TOEs, the evaluator shall examine the Guidance Documentation to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component.

Findings:	The TOE is not a distributed TOE.

188 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.

Findings:	The TOE uses published hashes.

2.5.5.3 Tests

189 The evaluator shall perform the following tests:

a. Test 1: The evaluator performs the version verification activity to determine the current version of the product. If a trusted update can be installed on the TOE with a delayed activation, the evaluator shall also query the most recently installed version (for this test the TOE shall be in a state where these two versions match). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. 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. 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.

High-Level Test Description
Get the current version of the TOE. Attempt to install a legitimate version of the TOE for the following circumstances: an upgrade. After the install, get the current version of the TOE and ensure it is consistent with the newly installed version.
Findings: PASS

b. 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:

1) A modified version (e.g. using a hex editor) of a legitimately signed update

2) An image that has not been signed

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)

4) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.

Findings:	The ST claims published hash.

c. Test 3 [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e., reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted. If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is 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.

1) The evaluator obtains or produces an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the implementation of the TOE, the TOE might not allow the user to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE

2) The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE. The evaluator confirms that this attempt fails. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the

verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE

3) If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.

Findings:	The TOE does not verify the update file.

190 If the verification of the hash value over the update file(s) against the published hash is not performed by the TOE, Test 3 shall be skipped.

191 The evaluator shall perform Test 1, Test 2, and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates).

Findings:	The ST claims published hash.

192 For distributed TOEs the evaluator shall perform Test 1, Test 2, and Test 3 (if applicable) for all TOE components.

Findings:	The TOE is not a distributed TOE.

2.6 TOE Access (FTA)

2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

2.6.1.1 TSS

193 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.

Findings:	[ST] section 6.1 – FTA_SSL_EXT.1 "If a local user session is inactive for a configured period of time, the session will be terminated". The evaluator confirmed that local session termination is supported with a configurable inactivity time setting.

2.6.1.2 Guidance Documentation

194 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.

Findings:	[AGD] section 4.5.2 specifies that session termination is used and provides the steps to configure the inactivity timeout. The CLI command to configure this is the "adminaccessconfig > timeout" function. This function affects the timeouts for all instances of the CLI (local and remote) and the remote Web UI.

2.6.1.3 Tests

195 The evaluator shall perform the following test:

a. Test 1: 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 re-authentication is needed when trying to unlock the session.

High-Level Test Description
Change the idle timeout to 5 minutes. Log into the device over the serial interface and SSH CLI interface. Wait for the full duration of the timeout without sending any keepalives. The session will terminate at exactly the configured time. Repeat the above steps for an 8minute timer.
Findings: PASS

2.6.2 FTA_SSL.3 TSF-initiated Termination

2.6.2.1 TSS

196 The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.

Findings:	[ST] section 6.1 – FTA_SSL.3 “the Authorized Administrator can specify how long a user can be logged into the Web Security appliance’s CLI before AsyncOS logs the user out due to inactivity.” The evaluator verified that the [ST] specifies remote session termination.

2.6.2.2 Guidance Documentation

197 The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.

Findings:	[AGD] section 4.5.2 indicates that the remote administrative sessions can be terminated after an idle period has elapsed. The CLI command to configure this is the “adminaccessconfig > timeout” function. This function affects the timeouts for all instances of the CLI (local and remote) and the remote Web UI.

2.6.2.3 Tests

198 For each method of remote administration, the evaluator shall perform the following test:

a. Test 1: 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.

High-Level Test Description
Change the idle timeout to 8 minutes. Log into the device over the Web UI. Wait for the full duration of the timeout without sending any keep-alives. The session should terminate. Repeat for a timeout value of 11 minutes. The SSH interface was tested in Test 1 for FTA_SSL_EXT.1 since the CLI timers affect both the serial and SSH CLIs.
Findings: PASS

2.6.3 FTA_SSL.4 User-initiated Termination

2.6.3.1 TSS

199 The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.

Findings:	[ST] section 6.1 – FTA_SSL.4 “An administrator is able to exit out of both the CLI and GUI administrative sessions. The Authorized Administrator can log out of the CLI with the 'exit' command.”

2.6.3.2 Guidance Documentation

200 The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.

Findings:	[AGD] section 4.5.3 specifies the Authorized Administrator can terminate their active sessions by clicking Logout on the Administrators GUI webpage or typing “exit” on the CLI.

2.6.3.3 Tests

201 For each method of remote administration, the evaluator shall perform the following tests:

a. Test 1: 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.

High-Level Test Description
Log into the serial console Log out using the TSFI previous discussed. Verify that the session has been terminated.
Findings: PASS

b. Test 2: 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.

High-Level Test Description
Log into the SSH interface and logout and show that the TOE is no longer connected. Log into the Web GUI interface. Copy the URL presented. Log out using the TSFI previous discussed. Paste the URL back into the web browser and attempt to navigate directly to it.
Findings: PASS

2.6.4 FTA_TAB.1 Default TOE Access Banners

2.6.4.1 TSS

202 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).

Findings:	[ST] section 6.1 – FTA_TAB.1 “The Authorized Administrator defines a custom login banner that will be displayed at the GUI and the CLI for both local and remote access.” The evaluator verified that the warning is displayed on all administrative methods of access.

2.6.4.2 Guidance Documentation

203 The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.

Findings:	[AGD] section 4.4 provides the steps to configure the login banner. This banner affects all interfaces simultaneously.

2.6.4.3 Tests

204 The evaluator shall also perform the following test:

a. Test 1: 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.

High-Level Test Description
Log into the CLI interface. Change the banner to a random string. Log into fresh sessions for all interactive interfaces and show that the banner was modified and is presented prior to I&A.
Findings: PASS

2.7 Trusted path/channels (FTP)

2.7.1 FTP_ITC.1 Inter-TSF trusted channel

2.7.1.1 TSS

205 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.

Findings:	The TOE acts as a client for providing logging messages over scp as described in section 6.1 of the [ST] under FTP_ITC.1. In section 6.1 of the [ST] under FCS_SSHC_EXT.1, the TSS describes that the scp connection to the remote entity is assured via the use of SSHv2 host keys (which employ public/private key cryptography). As there is only one trusted channel, it is trivial to map this function to the use of FCS_SSHC_EXT.1 SFR as described in section 6.1 of the [ST] under FCS_SSHC_EXT.1.

2.7.1.2 Guidance Documentation

206 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.

Findings:	[AGD] section 3.4 provides protocol and version (SSHV2) and a pointer to the online user guide section “Pushing Log Files to Another Server”. https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8/b_WSA_UserGuide_11_7_chapter_010101.html#task_1687223 The link provides the steps to configure communication with the audit server. This is a periodic connection which will reattempt connections should the connection be broken. If the SSH connection to the SCP server on a remote syslog server fails, the log files will remain on the TOE until the connection is restored. On the next SCP Push based on either the maximum log file size being exceeded or on the time interval, the current log file and the log files previously unsuccessfully transferred will be transferred.

2.7.1.3 Tests

207 The developer shall provide to the evaluator application layer configuration settings for all secure communication mechanisms specified by the FTP_ITC.1 requirement. This information should be sufficiently detailed to allow the evaluator to determine the application layer timeout settings for each cryptographic protocol. There is no expectation that this information must be recorded in any public-facing document or report.

208 The evaluator shall perform the following tests:

a. Test 1: 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.

Note	The TOE maintains trusted channels to the remote audit log which is set up as per the evaluated configuration. It is constantly tested throughout the evaluation.

b. Test 2: 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.

High-Level Test Description
Engage wireshark over the appropriate interface. Within the TOE, execute a log rollover on a log configured to transmit to the device we are watching with wireshark. Examine wireshark and verify that the TOE initiates SSH communications with the logging endpoint. Examine wireshark and verify that the traffic is encrypted.
Findings: PASS

c. Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Findings:	Refer to previous test

d. Test 4: 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.

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: i) a duration that exceeds the TOE's application layer timeout setting, ii) a duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer.

The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.

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.

High-Level Test Description
Configure the TOE to send logs once a minute. Indirectly disconnect the TOE from the switch and wait for the TOE to try to transmit logs to the disconnected endpoint. The TOE should report an error. Slow down the network using a bandwidth limiter and when the TOE starts a log rollover, (indirectly) disconnect the TOE from the switch and immediately reconnect. The TOE should continue sending traffic with only a minor pause. Slow down the network using a bandwidth limiter and when the TOE starts a log rollover, (indirectly) disconnect the TOE from the switch and wait until the TOE reports an error in the local logs.
Findings: PASS

Further assurance activities are associated with the specific protocols.

209 For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

Findings:	This is not a distributed TOE.

210 The developer shall provide to the evaluator application layer configuration settings for all secure communication mechanisms specified by the FTP_ITC.1 requirement. This information should be sufficiently detailed to allow the evaluator to determine the application layer timeout settings for each cryptographic protocol. There is no expectation that this information must be recorded in any public- facing document or report.

2.7.2 FTP_TRP.1/Admin Trusted Path

2.7.2.1 TSS

211 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.

Findings:	[ST] section 6.1 – FTP_TRP.1 “All remote administrative communications take place over a secure encrypted SSHv2 for the CLI or TLS/HTTPS for the GUI sessions.” This is consistent with the selections in section 5.2 of the [ST].

2.7.2.2 Guidance Documentation

212 The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.

Findings:	[AGD] section 3.3.2 specifics the steps to configure the TOE SSH server. [AGD] section 3.3.3 specifies the steps to configure the TOE TLS server. [AGD] section 1.5 specifies the use of a SSH client and HTTPS browser to connect to the TOE administrative interfaces.

2.7.2.3 Tests

213 The evaluator shall perform the following tests:

a. Test 1: 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.

Note	The only trusted paths are the SSH interface and web interface, which are both set up as per the evaluated configuration. They are constantly tested throughout the evaluation.

b. Test 2: The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.

High-Level Test Description
Engage wireshark over the appropriate interface. Log into the trusted path. Examine wireshark and verify that the trusted path sends encrypted traffic after any initial plaintext protocol negotiation occurs.
Findings: PASS

214 Further assurance activities are associated with the specific protocols.

215 For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.

Findings:	The TOE is not a distributed TOE.

3 Evaluation Activities for Optional Requirements

216 No optional requirements have been selected by this evaluation.

4 Evaluation Activities for Selection-Based Requirements

4.1 Cryptographic Support (FCS)

4.1.1 FCS_HTTPS_EXT.1 HTTPS Protocol

4.1.1.1 TSS

217 The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.

Findings:	Section 6.1 of the [ST] under FCS_HTTPS_EXT.1 states that the TOE is conformant with RFC 2818. RFC2818 provides guidance that servers should implement an RFC-conformant version of TLS, that the server should be able to negotiate TLS (either using a distinct port or through a connection upgrade feature) and that the server should offer an appropriate certificate to ensure clients can confirm the identity. The TSS information in the [ST] section 6.1 clearly indicates that a TLS connection is used (which is reliant on claiming FCS_TLSS_EXT.1 and requires an RFC-conformant TLS implementation). The TSS in section 6.1 of the [ST] also provides that the server has an X.509 certificate to offer to remote clients. The use of a distinct port is not a requirement of RFC 2818, though, we have confirmed through testing that the standard port 80 is closed and port 443 is active and only accepts TLS binary protocols.

4.1.1.2 Guidance Documentation

218 The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.

Findings:	[AGD] section 3.3.3 specifies the steps to configure the TOE TLS server.

4.1.1.3 Tests

219 This test is now performed as part of FIA_X509_EXT.1/Rev testing.

220 Tests are performed in conjunction with the TLS evaluation activities.

221 If the TOE is an HTTPS client or an HTTPS server utilizing X.509 client authentication, then the certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1.

4.1.2 FCS_SSHC_EXT.1 SSH Client

4.1.2.1 TSS

FCS_SSHC_EXT.1.2

222 The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list

conforms to FCS_SSHC_EXT.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described.

Findings:	Section 6.1 of the [ST] under FCS_SSHC_EXT.1 identifies the public key algorithms which are suitable for authenticating. The TOE does not offer password-based authentication to remote servers. The public key algorithms claimed in FCS_SSHC_EXT.1.5 are the *hostkey* algorithms which can differ from the algorithms offered by the TOE client to the remote server when used to identify and authenticate the client to the remote server. (For the purposes of FCS_SSHC_EXT.1 and TD0411 and TD0412, this AA is assumed to refer to the use of hostkey algorithms and not those offered for use by the TOE for identifying and authenticating to a remote server.) With that said, the [ST] in section 6.1 under FCS_SSHC_EXT.1 indicates that the TOE client will only negotiate ssh-rsa hostkeys and can offer ssh-rsa public keys for authentication to the remote server.

FCS_SSHC_EXT.1.3

223 The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 "SSH connections will be dropped if the TOE receives a packet larger than 256K bytes."

FCS_SSHC_EXT.1.4

224 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.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 "encryption algorithms, aes128-cbc, aes256-cbc, aes128-ctr and aes256-ctr to ensure confidentiality of the session." These encryption algorithms are identical to those listed for this component in section 5.2 of the [ST].

FCS_SSHC_EXT.1.5

225 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 "public key algorithms for authentication: rsa-sha2-256, rsa-sha2-512." These algorithms are identical to those listed for this component in section 5.2 of the [ST].

226 If x509v3-based public key authentication algorithms are claimed, the evaluator shall confirm that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate. For example, the TOE could verify that a server's configured IP address matches the one presented in the server's x.509v3 certificate.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 x509v3-based public key authentication algorithms are not claimed.

FCS_SSHC_EXT.1.6

227 The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that that list corresponds to the list in this component.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 “hashing algorithms HMAC-SHA1 to ensure the integrity of the session.” This algorithm is identical to the one listed for this component in section 5.2 of the [ST].

FCS_SSHC_EXT.1.7

228 The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that that list corresponds to the list in this component.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 “public key exchange: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.” These algorithms are identical to those listed for this component.

FCS_SSHC_EXT.1.8

229 The evaluator shall check that the TSS specifies the following:

1. Both thresholds are checked by the TOE.
2. Rekeying is performed upon reaching the threshold that is hit first.

Findings:	[ST] section 6.1 – FCS_SSHC_EXT.1 “A rekey occurs after a threshold of no longer than one hour and no more than one gigabyte of transmitted data.”

4.1.2.2 Guidance Documentation

FCS_SSHC_EXT.1.4

230 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).

Findings:	The TOE does not permit the cryptographic algorithms to be configured.

FCS_SSHC_EXT.1.5

231 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).

Findings:	The TOE does not permit the cryptographic algorithms to be configured.

FCS_SSHC_EXT.1.6

232 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).

Findings:	The TOE does not permit the integrity algorithms to be configured.

FCS_SSHC_EXT.1.7

233 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.

Findings:	The TOE does not permit the key exchange algorithms to be configured.

FCS_SSHC_EXT.1.8

234 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.

Findings:	The TOE does not permit the rekey thresholds to be configured.

4.1.2.3 Tests

FCS_SSHC_EXT.1.2

235 Test 1: If password-based authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server, and demonstrate that a Security Administrator can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.

Note: Public key authentication is tested as part of testing for FCS_SSHC_EXT.1.5

Findings:	The ST only claims public key mechanisms.

FCS_SSHC_EXT.1.3

236 The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

High-Level Test Description
Using a custom tool, transmit a packet larger than the expected TOE buffer size and show that the TOE rejects the packet in some way.
Findings: PASS

FCS_SSHC_EXT.1.4

237 The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish a SSH connection. To verify this, the evaluator shall start session establishment for a SSH connection with a remote server (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. 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.

High-Level Test Description
Permit the TOE client to connect to a test SSH server and capture the TOE client's advertised supported cipher algorithms. Verify that the advertised set matches the claimed set. Forcibly use an SSH server to permit connections from the TOE client using only one of those claimed ciphers and show that the connection is successful.
Findings: PASS

FCS_SSHC_EXT.1.5

238 Test 1: The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator shall therefore establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST.

High-Level Test Description
Use the TOE client and connect to a test SSH server which only permits the specified public key algorithms in turn. This requires the TOE to be loaded with a private key corresponding to the key pair and the non-TOE server to have access to the public key half.
Findings: PASS

239 Test 2: The evaluator shall configure an SSH server to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.

High-Level Test Description
Ensure the TOE has a supported host key for the TOE. Off-TOE, use a different private key (generated with an unsupported algorithm). Permit the TOE client to connect to the non-TOE server. The connection attempt should fail.
Findings: PASS

FCS_SSHC_EXT.1.6

240 Test 1: [conditional, if an HMAC or AEAD_AES_*_GCM 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.

241 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.

High-Level Test Description
Using an SSH Server, forcibly permit only the claimed integrity algorithms and show that connections by the TOE SSH client are accepted to form a successful connection.
Findings: PASS

242 Test 2: [conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST] The evaluator shall configure an SSH server to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails.

243 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.

High-Level Test Description
Using an SSH Server, forcibly permit an integrity algorithm which is not claimed by the TOE and show that a TOE SSH client connection results in a failed connection.
Findings: PASS

FCS_SSHC_EXT.1.7

244 Test 1: The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall attempt to connect from the TOE to the SSH server using each allowed key exchange method, and observe that each attempt succeeds.

High-Level Test Description
Using an SSH server, forcibly permit only one claimed key exchange mechanism at a time and show that the TOE client will successfully connect using that algorithm.
Findings: PASS

FCS_SSHC_EXT.1.8

245 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 traffic-based threshold.

246 For testing of the time-based threshold the evaluator shall use the TOE to connect to an SSH server 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).

247 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 server the TOE is connected to.

High-Level Test Description
Using a custom SSH server, use the TOE client to connect to the server and trickle data over the channel to avoid disconnection due to idle timeout. Ensure that the TOE rekeys before 1 hour has elapsed. Ensure that the TOE is responsible for sending the rekey initiation.
Findings: PASS

248 For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server 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_SSHC_EXT.1.8).

249 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).

250 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 server the TOE is connected to.

High-Level Test Description
Using a custom SSH server, permit the TOE client to connect to the server. The server will send large amounts of data over the channel back to the client. Ensure that the TOE rekeys before 1 GB in the aggregate has been transmitted. Ensure that the TOE is responsible for sending the rekey initiation.
Findings: PASS

251 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).

Findings:	The thresholds are not configurable.

252 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:

a) An argument is present in the TSS section describing this hardware-based limitation and

b) 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.

Findings:	The thresholds are not restricted by hardware limitations.

FCS_SSHC_EXT.1.9

253 Test 1: The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the Security Administrator to accept or deny the key before continuing the connection.

High-Level Test Description
Clear the known host key database. Using the TOE SSH client, connect to an SSH server and show that the TOE either warns the administrator that the host is unknown or that it rejects the connection attempt until after the host key has been manually added.
Findings: PASS

254 Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. If 'password-based' is selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords). If 'password-based' is not selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using public key-based authentication, and shall ensure that the TOE rejects the connection.

High-Level Test Description
Add a host key to the known hosts database either explicitly or implicitly depending on the mechanism for inserting the key. Generate a different host key for the non-TOE SSH server. Using the TOE SSH client, connect to the SSH server that advertises the wrong host key and show that the TOE rejects the connection. Verify public key authentication fails. The [ST] does not claim password-based authentication.
Findings: PASS

4.1.3 FCS_SSHS_EXT.1 SSH Server

4.1.3.1 TSS

FCS_SSHS_EXT.1.2

255 The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHS_EXT.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 specifies: "The TOE supports both public key-based and password-based authentication."

	"public key algorithms for authentication: rsa-sha2-256, rsa-sha2-512" The evaluator confirmed that the public key algorithms match those specified in FCS_SSHS_EXT.1.5.

FCS_SSHS_EXT.1.3

256 The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 "SSH connections will be dropped if the TOE receives a packet larger than 256K bytes."

FCS_SSHS_EXT.1.4

257 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.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 "encryption algorithms, aes128-cbc, aes256-cbc, aes128-ctr and aes256-ctr are used to ensure confidentiality of the session." These encryption algorithms are identical to those listed for this component in section 5.2 of the [ST].

FCS_SSHS_EXT.1.5

258 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 "public key algorithms for authentication: rsa-sha2-256, rsa-sha2-512." These algorithms are identical to those listed for this component in section 5.2 of the [ST].

259 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.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 "When establishing a connection to the SSH server using a public key, the public key is compared to the public key stored in the authorized_keys file. If the keys match, the connection is established."

FCS_SSHS_EXT.1.6

260 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.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 "hashing algorithms HMAC-SHA1 to ensure the integrity of the session." This algorithm is identical to the one listed for this component in section 5.2 of the [ST].

FCS_SSHS_EXT.1.7

261 The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that that list corresponds to the list in this component.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 “public key exchange: diffie-hellman-group14-sha1.” These algorithms are identical to those listed for this component in section 5.2 of the [ST].

FCS_SSHS_EXT.1.8

262 The evaluator shall check that the TSS specifies the following:

1. Both thresholds are checked by the TOE.

2. Rekeying is performed upon reaching the threshold that is hit first.

Findings:	[ST] section 6.1 – FCS_SSHS_EXT.1 “will be rekeyed after a threshold of no longer than one hour, and no more than one gigabyte of transmitted data.”

4.1.3.2 Guidance Documentation

FCS_SSHS_EXT.1.4

263 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).

Findings:	[AGD] section 3.3.2 provides instructions for configuring SSHv2.

FCS_SSHS_EXT.1.5

264 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).

Findings:	[AGD] section 3.3.2 provides instructions for configuring SSHv2.

FCS_SSHS_EXT.1.6

265 The evaluator shall also check the guidance documentation to ensure 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 (specifically, that the “none” MAC algorithm is not allowed).

Findings:	[AGD] section 3.3.2 provides instructions for configuring SSHv2.

FCS_SSHS_EXT.1.7

266 The evaluator shall also check the guidance documentation to ensure 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.

Findings:	[AGD] section 3.3.2 provides instructions for configuring SSHv2.

FCS_SSHS_EXT.1.8

267 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.

Findings:	[AGD] section 3.3.2 provides instructions for configuring SSHv2.

4.1.3.3 Tests

FCS_SSHS_EXT.1.2

268 Test 1: If password-based authentication methods have been selected in the ST then using the guidance documentation, 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 user.

NOTE:	Please refer to tests in FIA_UIA_EXT.1.

269 Test 2: If password-based authentication methods have been selected in the ST then the evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.

270 Note: Public key authentication is tested as part of testing for FCS_SSHS_EXT.1.5

NOTE:	Please refer to tests in FIA_UIA_EXT.1.

FCS_SSHS_EXT.1.3

271 The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

High-Level Test Description
Using a custom tool, transmit a packet larger than the expected TOE buffer size and show that the TOE rejects the packet in some way.
Findings: PASS

FCS_SSHS_EXT.1.4

272 The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish a SSH connection. To verify this, the evaluator shall start session establishment for a 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. 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.

High-Level Test Description
Using an SSH client, connect to the TOE server and capture the TOE server's advertised supported cipher algorithms. Verify that the advertised set matches the claimed set. Forcibly use a SSH client to connect using only one of those ciphers and show that the connection is successful.
Findings: PASS

FCS_SSHS_EXT.1.5

273 Test 1: The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

High-Level Test Description
Using an SSH client, connect to the TOE server using the specified public key algorithms in turn. This requires the TOE to be loaded with a public key corresponding to the key pair.
Findings: PASS

274 Test 2: The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize the 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. Test objective: The purpose of this negative test is to verify that the server rejects authentication attempts of clients that present a public key that does not match public key(s) associated by the TOE with the identity of the client (i.e. the public keys are unknown to the server). To demonstrate correct functionality, it is sufficient to determine that an SSH connection was not established after using a valid username and an unknown key of supported type.

High-Level Test Description
Load a supported public key into the TOE. Off-TOE, use a different private key (generated with the same public key algorithm) to try to connect. The connection attempt should fail.
Findings: PASS

275 Test 3: The evaluator shall configure an SSH client to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.

High-Level Test Description
Building upon the previous test case, attempt to log into the TOE using a private key from an unsupported algorithm and show the user fails to log in.
Findings: PASS

FCS_SSHS_EXT.1.6

276 Test 1: [conditional, if an HMAC or AEAD_AES_*_GCM 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.

277 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.

High-Level Test Description
Using an SSH client, forcibly negotiate only the claimed integrity algorithms and show that they are accepted to form a successful connection.
Findings: PASS

278 Test 2: [conditional, if an HMAC or AEAD_AES_*_GCM 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.

279 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.

High-Level Test Description
Using an SSH client, forcibly negotiate an integrity algorithm which is not claimed by the TOE and show that it results in a failed connection.
Findings: PASS

FCS_SSHS_EXT.1.7

280 Test 1: 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.

High-Level Test Description
Using an SSH client, forcibly negotiate the diffie-hellman-group1-sha1 key exchange algorithm which is not supported by the TOE and show that it results in a failed connection.
Findings: PASS

281 Test 2: 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.

High-Level Test Description
Using an SSH client, forcibly negotiate each of the claimed key exchange algorithms in turn and show that it results in a successful connection.
Findings: PASS

FCS_SSHS_EXT.1.8

282 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 traffic-based threshold.

283 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).

284 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.

High-Level Test Description
Using a custom SSH client, connect to the TOE and trickle data over the channel to avoid disconnection due to idle timeout. Ensure that the TOE rekeys before 1 hour has elapsed. Ensure that the TOE is responsible for sending the rekey initiation.
Findings: PASS

285 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).

286 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).

287 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.

High-Level Test Description
Using a custom SSH client, connect to the TOE and send large amounts of data over the channel. Ensure that the TOE rekeys before 1 GB in the aggregate has been transmitted. Ensure that the TOE is responsible for sending the rekey initiation.
Findings: PASS

288 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).

Findings:	The thresholds are not configurable.

289 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:

a. An argument is present in the TSS section describing this hardware-based limitation and

b. 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.

Findings:	The thresholds are not restricted by hardware limitations.

4.1.4 FCS_TLSS_EXT.1 Extended: TLS Server Protocol without mutual authentication

4.1.4.1 TSS

FCS_TLSS_EXT.1.1

290 The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

Findings:	[ST] section 6.1 – FCS_TLSS_EXT.1 the list of ciphersuites included matches those selected in the component.

FCS_TLSS_EXT.1.2

291 The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.

Findings:	[ST] section 6.1 – FCS_TLSS_EXT.1 “Once configured, the TOE will not establish TLS v1.0, SSL2.0 or SSL3.0 connections if offered by the client”.

FCS_TLSS_EXT.1.3

292 If using ECDHE or DHE ciphers, the evaluator shall verify that the TSS describes the key agreement parameters of the server Key Exchange message.

Findings:	[ST] section 6.1 – FCS_TLSS_EXT.1 “Both RSA 2048 and ECDHE using secp 256r1 are being used for key exchange and authentication.”

FCS_TLSS_EXT.1.4

293 The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).

Findings:	[ST] section 6.1 specifies that the “TOE supports TLS session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2) and session resumption based on session tickets according to RFC 5077”.

294 If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.

Findings:	[ST] section 6.1 specifies that the “Session tickets are encrypted using AESCBC-128- and AESGCM-256”.

295 If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.

296 [TD0569] If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.

Findings:	[ST] section 6.1 specifies that "session resumption based on session tickets according to RFC 5077."

4.1.4.2 Guidance Documentation

FCS_TLSS_EXT.1.1

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

Findings:	[AGD] section 3.3.3 provides instructions for configuring TLS. This includes limiting the ciphersuites used.

FCS_TLSS_EXT.1.2

298 The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.

Findings:	[AGD] section 3.3.3 provides instructions for configuring TLS. This includes limiting the protocol versions used.

FCS_TLSS_EXT.1.3

299 The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.

Findings:	[AGD] section 3.3.3 provides instructions for configuring TLS. This includes limiting the ciphersuites used.

[TD0569] FCS_TLSS_EXT.1.4

300 The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.

Findings:	[AGD] section 3.3.3 provides instructions for configuring TLS. This includes limiting the ciphersuites used.

4.1.4.3 Tests

FCS_TLSS_EXT.1.1

301 Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is

sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using the claimed ciphersuites.
Findings: PASS

302 Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using an unsupported ciphersuite. Then connect to the TOE using TLS_NULL_WITH_NULL_NULL.
Findings: PASS

303 Test 3: The evaluator shall perform the following modifications to the traffic:

a. Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE, and modify the first payload byte in the Client Finished message.
Findings: PASS

b. (Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.)

The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent.

The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished

message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.

High-Level Test Description
Perform a successful handshake using one of the accepted ciphersuites and verify that the Server Finished message is encrypted.
Findings: PASS

FCS_TLSS_EXT.1.2

304 The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.

High-Level Test Description
Using a Lightship developed TLS client, attempt to connect to the TOE and negotiate SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. The TOE denied connections with TLS protocol versions SSL 2.0, SSL 3.0, and TLS 1.0 as expected.
Findings: PASS

FCS_TLSS_EXT.1.3

305 Test 1: [conditional] If ECDHE ciphersuites are supported:

a) The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using a valid ECDHE ciphersuite and verify that the size of the Server Key Exchange message matches the expected bit size for the chosen ECDH parameter.
Findings: PASS

b) The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g., secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using a valid ECDHE ciphersuite and verify that the TOE rejects the connection.
Findings: PASS

306 Test 2: [conditional] If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).

NOTE:	DHE ciphersuites are not claimed in the [ST].

307 Test 3: [conditional] If RSA key establishment ciphersuites are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE using a valid pure RSA ciphersuite and verify that the certificate that comes back from the Server Certificate message matches the expected bit size.
Findings: PASS

FCS_TLSS_EXT.1.4

308 Test Objective: To demonstrate that the TOE will not resume a session for which the client failed to complete the handshake (independent of TOE support for session resumption).

309 Test 1 [conditional]: If the TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077, the evaluator shall perform the following test:

a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket.
b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake).
c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps:
Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID.
d) The client completes the TLS handshake and captures the SessionID from the ServerHello.

e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d).

f) The client verifies the TOE (1) implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.

310 [TD0569] Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.

NOTE:	Session tickets and session IDs are both claimed in the [ST].

311 Test 2 [conditional]: If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):

a) The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246).

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE in a valid manner and capture the session ID. Resume the session using the session ID and verify the resumption is successful without a full TLS handshake.
Findings: PASS

b) The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.

312 [TD0569] Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ID may be obtained in one context for resumption in another context. There is no requirement that the session ID be obtained and replayed within the same context subject to the description provided in the TSS. All

contexts that can reuse a session ID constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE in manner to cause a fatal alert and capture the session ID. Attempt to resume the session using the session ID and verify the resumption fails.
Findings: PASS

313 Test 3 [conditional]: If the TOE supports session tickets according to RFC5077, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):

a) [TD0556] The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with an abbreviated handshake described in section 3.1 of RFC 5077 and illustrated with an example in figure 2. Of particular note: if the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello in the abbreviated handshake (which is shown in figure 2). This is not required, however as further clarified in section 3.3 of RFC 5077.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE in a valid manner and capture the session ticket. Resume the session using the session ticket and verify the resumption is successful without a full TLS handshake.
Findings: PASS

b) The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.

314 [TD0569] Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ID may be obtained in one context for resumption in another context. There is no requirement that the session ID be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ID constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.

High-Level Test Description
Using a Lightship developed TLS client, connect to the TOE in a valid manner and capture the session ticket. The Lightship developed TLS client with then modify the session ticket and attempt

High-Level Test Description
to resume the session with the modified session ticket. Verify that the session resumption does not occur.
Findings: PASS

4.2 Identification and Authentication (FIA)

4.2.1 FIA_X509_EXT.1/Rev X.509 Certificate Validation

4.2.1.1 TSS

315 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).

Findings:	[ST] section 6.1 – FIA_X509_EXT.1/Rev "The certificate validation checking takes place during the TLS session setup and when a certificate is loaded." The section also lists the rules for extended key usage. The TOE does not support the use of peer certificates and only validates its own certificate. The TOE supports revocation checking of its own certificate.

316 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.

Findings:	[ST] section 6.1 – FIA_X509_EXT.1/Rev "Prior to being loaded into the TOE, all certificates are validated against a revocation list using OCSP."

4.2.1.2 Guidance Documentation

317 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.

Findings:	[AGD] section 3.3.4 provides instructions for loading a certificate onto the TOE including the verification of a signed CSR. This is the only type of validation the TOE performs on certificates. This section also provides information on certificate revocation.

4.2.1.3 Tests

318 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.1.1/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:

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)

   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.

High-Level Test Description
Attempt to load a certificate onto the TOE with a valid root, and intermediate CA certificates. Verify that the leaf certificate can be loaded onto the TOE. Delete all loaded certificates and then attempt to load a certificate onto the TOE without a root CA certificate and with a valid intermediate CA certificate. Verify that the leaf certificate is rejected when an attempt to load it is made. Delete all loaded certificates and then attempt to load a certificate onto the TOE with a valid root CA certificate and without an intermediate CA certificate. Verify that the leaf certificate is rejected when an attempt to load it is made.
Findings: PASS

b. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.

High-Level Test Description
Create a trust anchor with a ‘notAfter’ date in the past. Attempt to load this certificate into the TOE and show it is not accepted. Create an intermediate certificate with a ‘notAfter’ date in the past. Attempt to load this certificate into the TOE and show it is not accepted. Create a leaf certificate with a ‘notAfter’ date in the past. Attempt to load this certificate into the TOE and show it is not accepted.
Findings: PASS

c. 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. 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.

High-Level Test Description
Force the TOE to use an OCSP responder containing a revoked server certificate. Show that attempting to load the server certificate fails. Force the TOE to use an OCSP responder containing a revoked intermediate certificate. Show that attempting to load the server certificate fails.
Findings: PASS

d. Test 4: 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.

High-Level Test Description
Load the CA into the TOE trust store. Create an OCSP signing certificate using a known good CA certificate that has the OCSPSigning extendedKeyUsage flag enabled. Clone the known good CA certificate and **remove** the OCSPSigning extendedKeyUsage. The OCSP signature only depends on the (cloned) private key of the CA used to sign it and the TOE does not engage in any certificate pinning. Replace the old CA with the newly cloned CA. Verify the connection now fails due to the OCSP response being signed by a CA without the proper flag.
Findings: PASS

e. Test 5: 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.)

High-Level Test Description
Attempt to load a mangled leaf certificate into the trust store and show that this fails.
Findings: PASS

f. 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.)

High-Level Test Description
Attempt to load a mangled X.509 certificate in which the last byte has been modified. Verify the attempt is rejected.
Findings: PASS

g. 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.)

High-Level Test Description
Attempt to load a mangled X.509 certificate in which the public key has been modified. Verify the attempt is rejected.
Findings: PASS

h. [TD0527] Test 8: (Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen). The evaluator shall conduct the following tests:

Test 8a: (Conditional on TOE ability to process CA certificates presented in certificate message) 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.

Test 8b: (Conditional on TOE ability to process CA certificates presented in certificate message) 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.

Test 8c: 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.

NOTE:	The ST does not claim EC certificates in FCS_COP.1/SigGen.

319 The evaluator shall perform the following tests for FIA_X509_EXT.1.2/Rev. 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.

320 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).

321 For each of the following tests the evaluator shall create a chain of at least three certificates: a self-signed root CA certificate, an intermediate CA certificate and a leaf (node) certificate. 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).

a. 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: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) 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).

High-Level Test Description
Attempt to load a CA certificate into the trust store which is missing the basicConstraints extension. Show that the attempt to load fails.
Findings: PASS

b. 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: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) 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).

High-Level Test Description
Attempt to load a CA certificate into the trust store which has a basicConstraints extension CA flag set to False. Show that the attempt to load fails.
Findings: PASS

322 The evaluator shall repeat these tests for each distinct use of certificates. Thus, for example, use of certificates for TLS connection is distinct from use of certificates for trusted updates so both of these uses would be tested. But there is no need to repeat the tests for each separate TLS channel in FTP_ITC.1 and FTP_TRP.1/Admin (unless the channels use separate implementations of TLS).

Findings:	All distinct use of certificates have been covered.

4.2.2 FIA_X509_EXT.2 X.509 Certificate Authentication

4.2.2.1 TSS

323 The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates.

Findings:	[ST] section 6.1 – FIA_X509_EXT.2 The TOE supports a certificate chain which leads to the TOE certificate. This certificate chain is used to validate the TOE certificate. There are no certificates in operating environment for the TOE.

324 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.

Findings:	[ST] section 6.1 – FIA_X509_EXT.2 "If the connection to determine the certificate validity cannot be established, WSA does not accept the certificate."

4.2.2.2 Guidance Documentation

325 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.

Findings:	[AGD] section 3.3.4 provides instructions for loading a certificate onto the TOE including the verification of a signed CSR. This is the only type of validation the TOE performs. The TOE does not validate peer certificates for trusted channel as it only uses SSH for outbound connections.

4.2.2.3 Tests

326 The evaluator shall perform the following test for each trusted channel:

327 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. 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. 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.

High-Level Test Description
Start the OCSP responder for both the leaf and intermediate certificates and attempt to load the certificate chain onto the TOE. Verify that the TOE will accept the attempt to load the certificates. Stop the OCSP responders and attempt to load the certificate chain onto the TOE. Verify that the TOE will reject the attempt to load the certificates.
Findings: PASS

4.2.3 FIA_X509_EXT.3 Extended: X509 Certificate Requests

4.2.3.1 TSS

328 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.

Findings:	[ST] section 6.1 – FIA_X509_EXT.3 device-specific information is not selected.

4.2.3.2 Guidance Documentation

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.

Findings:	[AGD] section 3.3.4 provides instructions generating a CSR including the entry of the fields.

4.2.3.3 Tests

329 The evaluator shall perform the following tests:

a. Test 1: 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.

High-Level Test Description
Using the web interface, construct a new X.509 CSR, download it and show that it contains the necessary information required by the SFR.
Findings: PASS

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 certificate response message and demonstrate that the function succeeds.

High-Level Test Description
Attempt to load a signed certificate response without the associated trust chain. Show that the certificate fails to be imported. Load the trust anchor and any intermediate certificates into the trust store. Upload the signed certificate response and show that the attempt is successful.
Findings: PASS

4.3 Security management (FMT)

4.3.1 FMT_MOF.1/Functions Management of security functions behaviour

4.3.1.1 TSS

330 For distributed TOEs see chapter 2.4.1.1.

Findings:	The TOE is not a distributed TOE.

331 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).

Findings:	[ST] section 6.1 – FMT_MOF.1/Functions “Through the CLI, the TOE provides the ability for Authorized Administrators to manage TOE data, such as audit data to include transmission of audit data to a remote syslog server”.

4.3.1.2 Guidance Documentation

332 For distributed TOEs see chapter 2.4.1.2.

Findings:	The TOE is not a distributed TOE.

333 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.

Findings:	[AGD] section 3.4 provides instructions for configuring the logging service.

4.3.1.3 Tests

334 Test 1 (if ‘transmission of audit data to external IT entity’ is selected from the second selection together with 'modify the behaviour of' 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.

Findings:	This function is not selected.

335 Test 2 (if ‘transmission of audit data to external IT entity’ is selected from the second selection together with 'modify the behaviour of' 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.

336 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.

Findings: This function is not selected.

337 Test 1 (if 'handling of audit data' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data 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 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. The term ‘handling of audit data’ refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.

Findings: This function is not selected.

338 Test 2 (if 'handling of audit data' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term ‘handling of audit data’ refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.

339 The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.

Findings: This function is not selected.

340 Test 1 (if 'audit functionality when Local Audit Storage Space is full' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full without prior authentication as Security Administrator (by authentication as_a user with no administrator privileges or without user authentication at all). This attempt 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 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.

Findings: This function is not selected.

341 Test 2 (if 'audit functionality when Local Audit Storage Space is full' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full with prior authentication as Security Administrator. This attempt should be successful. The effect of the change shall be verified.

342 The evaluator does not necessarily have to test all possible values for the behaviour when Local Audit Storage Space is full but at least one change between allowed values for the behaviour.

Findings:	This function is not selected.

343 Test 3 (if in the first selection 'determine the behaviour of' has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall 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 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.

High-Level Test Description
As a privileged administrator, attempt to view the log transfer settings using the CLI and show the attempt is successful. As an unprivileged administrator, attempt to view the log transfer settings using the CLI and show the attempt is unsuccessful. As a privileged administrator, attempt to view the log transfer settings using the Web GUI and show the attempt is successful. Copy the URL for the log transfer settings. As an unprivileged administrator, attempt to view the log transfer settings using the CLI and show the attempt is unsuccessful. Paste the URL for the log transfer settings into the Web UI and show that direct navigation is not successful.
Findings: PASS

344 Test 4 (if in the first selection 'determine the behaviour of' has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with administrator authentication shall be successful.

Findings:	Please refer to previous test case.

4.3.2 FMT_MTD.1/CryptoKeys Management of TSF Data

4.3.2.1 TSS

345 For distributed TOEs see chapter 2.4.1.1.

Findings:	The TOE is not a distributed TOE.

346 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.

Findings:	[ST] section 6.1 – FMT_MTD.1/CryptoKeys “Through the CLI, the TOE provides the ability for Authorized Administrators to manage TOE data, such as audit data to include transmission of audit data to a remote syslog server, configuration settings, cryptographic keys, security attributes and login banners via the CLI and GUI.”

4.3.2.2 Guidance Documentation

347 For distributed TOEs see chapter 2.4.1.2.

Findings:	The TOE is not a distributed TOE.

348 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.

Findings:	[AGD] section 3.3.4, 3.3.5, and 3.3.6 provide instructions for generating keys via generating a CSR and the management of certificates. Section 3.3.2 specifies that the hostkeyconfig command is used to generate the SSH server keys.

4.3.2.3 Tests

349 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.

350 The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.

High-Level Test Description
As a non-privileged administrator, attempt to generate a new public/private key pair and show the operation is not permitted. Use of the privileged administrator to execute the same is done in FIA_X509_EXT.1/Rev.
Findings: PASS

5 Evaluation Activities for Security Assurance Requirements

5.1 ASE: Security Target

351 When evaluating a Security Target, the evaluator performs the work units as presented in the CEM. In addition, the evaluator ensures the content of the TSS in the ST satisfies the EAs specified in Section 2 (Evaluation Activities for SFRs).

Findings:	See above sections.

352 For distributed TOEs only the SFRs classified as 'all' have to be fulfilled by all TOE parts. The SFRs classified as 'One' or 'Feature Dependent' only have to be fulfilled by either one or some TOE parts, respectively. To make sure that the distributed TOE as a whole fulfills all the SFRs the following actions for ASE_TSS.1 have to be performed as part of ASE_TSS.1.1E.

ASE_TSS.1 element	Evaluator Action
ASE_TSS.1.1C	The evaluator shall examine the TSS to determine that it is clear which TOE components contribute to each SFR or how the components combine to meet each SFR. The evaluator shall verify the sufficiency to fulfil the related SFRs. This includes checking that the TOE as a whole fully covers all SFRs and that all functionality that is required to be audited is in fact audited regardless of the component that carries it out.

Findings:	The TOE is not a distributed TOE.

5.2 ADV: Development

353 The design information about the TOE is contained in the guidance documentation available to the end user as well as the TSS portion of the ST, and any required supplementary information required by this cPP that is not to be made public.

354 The functional specification describes the TOE Security Functions Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces.

355 No additional "functional specification" documentation is necessary to satisfy the Evaluation Activities specified in [SD].

356 The Evaluation Activities in [SD] are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

357 5.2.1.1 Evaluation Activity: 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.

Findings:	From section 7.2.1 of the NDcPP : "For this cPP, the Evaluation Activities for this family focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation." The [ST] and the AGD comprise the functional specification. If the test in [SD] cannot be completed because the [ST] or the AGD are incomplete, then the functional specification is not complete and observations are required. During the evaluator's use of the product and its interfaces (the Web GUI, SSH CLI, local serial port), there were no areas that were deficient.

358 5.2.1.2 Evaluation Activity: 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.

Findings:	See comments in the previous work unit.

359 5.2.1.3 Evaluation Activity: The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

Findings:	See comments in the previous work unit.

5.3 AGD: Guidance

360 The design information about the TOE is contained in the guidance documentation available to the end user as well as the TSS portion of the ST, and any required supplementary information required by this cPP that is not to be made public.

361 5.3.1.1 Evaluation Activity: 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.

Findings:	The documentation is available for public download from Cisco's web site (https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-8/user_guide/b_WSA_UserGuide_11_8.html).

362 5.3.1.2 Evaluation Activity: 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.

Findings:	All TOE platforms claimed in [ST] are covered by the operational guidance. This is evidenced by the platform equivalency.

363 5.3.1.3 Evaluation Activity: 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.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement.

364 5.3.1.4 Evaluation Activity: 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.

Findings:	[AGD] section 3.3 specifies the interfaces used by the TOE in the evaluated configuration.

365 5.3.1.5 Evaluation Activity

366 In addition the evaluator shall ensure that the following requirements are also met.

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.

[TD0536] 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::

1) 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).

2) 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.

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.

Findings:	[AGD] section 3.2.1 provides instructions for configuring FIPS mode which addresses this requirement. [AGD] sections 2 and 4.7 provide instructions for the download and verification of the TOE updates. [AGD] section 1.6 provides a list of excluded functions.

367 5.3.2.1 Evaluation Activity: The evaluator shall examine 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 (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).

Findings:	[AGD] section 1.5 provides instructions for configuration of the Operational Environment.

368 5.3.2.2 Evaluation Activity: 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.

Findings:	[AGD] section 1.5 provides instructions for configuration of the Operational Environment. The evaluator verified that this addresses all claimed platforms.

369 5.3.2.3 Evaluation Activity: The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.

Findings:	[AGD] section 2 provides instructions for the secure installation of the TOE. This covers all claimed Operational Environments.

370 5.3.2.4 Evaluation Activity: 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.

Findings:	The guidance documentation provides extensive information on managing the security of the TOE as an individual product. Additional best practice guidance provided within those documents helps instill a culture of secure manageability within a larger operational environment.

371 5.3.2.5 Evaluation Activity: 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.

Findings:	The [AGD] section 2 specifies the secure installation of the TOE to provide a protected interface. The online user guide referenced by the [AGD] provides the default password.

6 Vulnerability Assessment

372 5.6.1.1 Evaluation Activity: The evaluator shall examine the documentation outlined below provided by the developer to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.

373 [TD0547] The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside of the TOE), for example a web server, protocol, or cryptographic libraries, (independently identifiable and reusable components are not limited to the list provided in the example). This additional documentation is merely a list of the name and version number of the components and will be used by the evaluators in formulating vulnerability hypotheses during their analysis.

Findings:	The evaluator collected this information from the developer which was used to feed into the Type 1 Flaw Hypotheses search (below).

374 5.6.1.2 Evaluation Activity: The evaluator formulates hypotheses in accordance with process defined in Appendix A. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3.

Findings:	The following sources of public vulnerabilities were considered in formulating the specific list of flaws to be investigated by the evaluators, as well as to reference in directing the evaluators to perform key-word searches during the evaluation of the TOE. Hypothesis sources for public vulnerabilities were: Vendor security advisories: https://tools.cisco.com/security/center/publicationListing.x NIST National Vulnerability Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search CVE Details: https://www.cvedetails.com/ OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html OpenSSH Release Notes: https://www.openssh.com/releasenotes.html Google Type 1 Hypothesis searches were conducted on August 17, 2021, and included the following search terms: Web Security Appliance S190, S195, S380, S390, S395, S680, S690, S690X, S695, S695F Cisco AsyncOS 11.8 Glass web server

OpenSSH

OpenSSL

The evaluation team determined no residual vulnerabilities exist based on these searches that are exploitable by attacker.

There are no type-2 hypotheses identified for the NDcPP.

The evaluation team developed Types 3 and 4 flaw hypotheses in accordance with Sections A.1.3, A.1.4, and A.2 (of the SD), and that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential in accordance with the guidance in the CEM.