Supporting Document
Mandatory Technical Document

PP-Module for SSL/TLS Inspection Proxies
Version: 1.1
2021-09-10
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.1	2021-09-10	Updates to reflect Github conversion, compatibility with NDcPP v2.2E, and Technical Decisions applied to version 1.0
1.0	2019-08-23	Update release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of SSL/TLS Inspection Proxies products.

Acknowledgements:
This SD was developed with support from NIAP SSL/TLS Inspection Proxies Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for SSL/TLS Inspection Proxies is to describe the security functionality of SSL/TLS Inspection Proxies products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Protection Profile for General Purpose Operating Systems, Version

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- SSL/TLS Inspection Proxies, Version 1.1

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activites to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

The following sections list Common Criteria and technology terms used in this document.

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.
Target of Evaluation (TOE)	The product under evaluation.

1.3.2 Technical Terms

Attribute	A characterization of an entity (monitored client or the server requested by a monitored client) used in the TLS session establishment policy or the plaintext processing policy implemented by the TOE that describes the entity. Common attributes include IP address, name, and certificates associated to an entity.
	A high-level operation of the TLS session establishment policy implemented by the TOE

Block operation	that prevents TLS sessions between a monitored client and the server requested by the client.
Bypass operation	A high-level operation of the TLS session establishment policy implemented by the TOE that allows a TLS session between a monitored client and the server requested by the client. Alternatively, an operation of the plaintext processing policy implemented by the TOE to bypass certain inspection processing functional components for plaintext data flows established under the SSL/TLS session establishment policy.
Inspect operation	A high-level operation of the TLS session establishment policy implemented by the TOE that establishes a TLS session thread between a monitored client and a server requested by the monitored client in order to provide security services on the underlying plaintext application data.
Inspection processing functional components	A discrete set of security functions implemented within a single logical component, internal or external to the TOE that provides security services based on a plaintext data flow controlled by the TOE intended to protect a monitored client from defined security threats, or to enforce a defined policy regarding the servers allowed to be accessed by monitored clients.
Monitored Client	A TLS client that uses the TOE as an SSL/TLS Inspection Proxy. This device requires a trust anchor to be installed for the internal CA of the TOE, and makes SSL/TLS requests for services external to the enclave. This client makes SSL/TLS requests to a “requested server” through the TOE.
Requested Server	The target of an SSL/TLS request by a monitored client through the TOE. It is typically a service provider for clients using SSL/TLS. If mutual authentication is to be supported, this device requires a trust anchor to be installed for the internal CA of the TOE.
Secure Sockets Layer/Transport Layer Security (SSL/TLS)	A set of security protocols defined by IETF RFCs to establish a secure point-to-point channel between a client and a server. The secure channel provides confidentiality, integrity and proof of origin to plaintext application data transferred between the client and server. SSL refers to early implementations of the SSL/TLS protocols that are deprecated. TLS refers to current versions of the SSL/TLS protocol.
TLS messages	Specific messages defined by TLS protocol standards. The TLS messages addressed in this PP-Module include TLS handshake messages: Client Hello, Server Hello, Server Certificate, Server Key Exchange, Client Key Exchange, Certificate Request, Client Certificate, Client Certificate Verify, Server Finished and Client Finished messages.
TLS session parameters	The parameters of a TLS session established by the TOE for protecting thrutraffic, minimally to include: the negotiated version, negotiated cipher suite, the size of any key exchange values sent or received in key exchange messages, the server certificate received, (a reference to) the server certificate sent, the client certificate received, (a reference to) the client certificate sent, and other negotiated values determined by the TLS handshake that are not fixed for all TLS sessions established.
TLS session thread	A connection negotiated by the TOE consisting of a TLS secure point-to-point channel between a monitored client and the TOE, a TLS secure point-to-point channel between the TOE and the requested server, and any traffic flow containing the underlying application plaintext decrypted from one of the SSL/TLS channels, that is transferred within or between inspection processing functional components controlled by the TOE.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labelled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator’s verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator’s verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labelled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have

existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer’s tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Protection Profile for General Purpose Operating Systems

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the General Purpose Operating Systems PP.

2.1.1 Modified SFRs

2.1.1.1 Security Audit (FAU)

Other than this SFR becoming mandatory versus optional, there is no modification to this SFR. This PP-Module does not modify this SFR as it is defined in the Base-PP. This SFR is optional in the Base-PP but is mandatory for a TOE that conforms to this PP-Module. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

2.1.1.2 Cryptographic Support (FCS)

The ST author is instructed to include security critical parameters and when key destruction is required. The TSF shall destroy all cryptographic keys and critical security parameters, when no longer required in accordance with the specified cryptographic key destruction method For plaintext keys in volatile storage, the destruction shall be executed by a Single overwrite consisting of a pseudo-random pattern using the TSF's RBG zeroes ones a new value of the key a static or dynamic value that does not contain any CSP Destruction of reference to the key directly followed by a request for garbage collection For plaintext keys in non-volatile storage, the destruction shall be executed the invocation of an interface provided by a part of the TSF that Logically addresses the storage location of the key and performs a singlenumber of passes-pass overwrite consisting of a pseudo-random pattern using the TSF's RBG zeroes ones a new value of the key a static or dynamic value that does not contain any CSP Instructs a part of the TSF to destroy the abstraction that represents the key that meets the following: [no standard]. This SFR is refined from its definition in the Base-PP through the inclusion of security critical parameters and clarifies when destruction is required; a STIP device includes persistent keys, including the embedded CA’s signing private key that should not be destroyed until they are no longer needed. Security critical parameters includes security related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CA or the security of the information protected by the CA or the security of the information protected by the CA. This SFR is refined in this PP-Module to include requirementsfor destruction of security critical parameters as well as keys. The EA for the Base-PP are extended to include security critical parameters whenever keys are indicated. Other than this SFR becoming mandatory versus selection-based, there is no modification to this SFR. This PP-Module does not modify this SFR as it is defined in the Base-PP. This SFR is selection-based in the Base-PP but is mandatory for a TOE that conforms to this PP-Module because of this PP-Module's modifications to FTP_ITC.1. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed. Other than this SFR becoming mandatory versus selection-based, there is no modification to this SFR. This PP-Module does not modify this SFR as it is defined in the Base-PP. This SFR is selection-based in the Base-PP but is mandatory for a TOE that conforms to this PP-Module because of this PP-Module's modifications to FTP_ITC.1. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4
This SFR is refined in this PP-Module to include requirementsfor destruction of security critical parameters as well as keys. The EA for the Base-PP are extended to include security critical parameters whenever keys are indicated.

FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

2.1.1.3 Identification and Authentication (FIA)

Other than this SFR becoming mandatory versus selection-based, there is no modification to this SFR. This PP-Module does not modify this SFR as it is defined in the Base-PP. This SFR is selection-based in the Base-PP but is mandatory for a TOE that conforms to this PP-Module because of this PP-Module's modifications to FTP_ITC.1. FIA_X509_EXT.1/STIP defines the TOE's X.509 validation behavior for TLS certificates presented to the TSF as part of TLS proxying. At minimum, FIA_X509_EXT.1/Rev is used by the TOE to validate any certificates loaded onto it. If the TOE has other functions that require the use of X.509 certificates (e.g. code signing for integrity testing or software updates, TLS interfaces used for a purpose other than session proxying such as audit server or authentication server connections), FIA_X509_EXT.1/Rev applies to those as well. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed. The PP-Module partially completes selections in this SFR using the available options to specify minimum required functionality for X.509 authentication based on its use in STIP. The PP-Module also refines the authorized management roles that can perform the function defined in FIA_X509_EXT.2.2. The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS, DTLS HTTPS IPsec SSH no other protocols and code signing for system software updates code signing for integrity verification other uses no additional uses . When the TSF cannot establish a connection to determine the revocation status of a certificate, the TSF shall allow the Security Administrator CA Operations Staff to choose whether to accept the certificate associate the failed connection event per FDP_TEP_EXT.1.5 in these cases accept the certificate not accept the certificate . “TLS” is moved outside the selection in the first element, since the TOE must implement TLS to accomplish the STIP functionality. The application notes for the first element from the Base-PP also apply. It is worth noting that since this SFR applies to all uses of certificates in the TOE, it may be the case that the actions taken in response to a failure to be able to determine revocation status (which is specified in the 2nd element) is handled differently for different connections. If this is the case, the ST author must make it clear which actions are associated with which connections so that the correct evaluation of the functionality can be performed. The second element has three modifications from that in the Base-PP. First, the word “validity” is replaced with “revocation status” for clarity. This is consistent with what is in the application note in the NDcPP, and using “revocation status” more directly indicates what is required. Second, the general notion of “administrator” is replaced with the more refined roles defined in this PP-Module; the ST author should make the appropriate selection. Finally, a selection is added that allows ST author flexibility in addressing the issue of failure to connect to check revocation status in the specific case that the certificates being checked are associated with either a monitored client or a requested server. This selection (“to associate the failed connection event per FDP_TEP_EXT.1.5”), when chosen, indicates that selected administrative role is able to specify a STIP operation (block, bypass, inspect) to be taken in the event that the revocation status can’t be checked. The requirement that the TOE be able to perform this operation when such an event occurs is specified in FDP_TEP_EXT.1.5. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed. There is no change to this SFR. Only its trigger for inclusion is changed because this PP-Module introduces an alternate method of obtaining a certificate for the TOE. In the Base-PP, this SFR is optional but must be claimed in any situation where the TOE presents its own X.509 certificate to an external entity (e.g. any case where the TOE acts as a TLS server or where the TOE acts as a TLS client in an connection that uses mutual authentication). A STIP TOE must present an X.509 certificate to an external entity as part of TLS session proxying. The TOE may obtain this certificate either using PKCS#10 (covered by this SFR) or through Enrollment over Secure Transport (EST), which is covered by the selection-based SFR FIA_ESTC_EXT.1. Therefore, the ST author only claims FIA_X509_EXT.3 if PKCS#10 is selected in FIA_ENR_EXT.1. There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1/Rev
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

2.1.1.4 Trusted Path/Channels (FTP)

The PP-Module partially completes selections and assignments in this SFR using the available options to specify external interfaces and trusted channels that all STIP products must support at minimum. The TSF shall be capable of using TLS and IPsec SSH DTLS HTTPS no other protocols to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, TLS session proxying, authentication server other capabilities no other capabilities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel. The TSF shall initiate communication via the trusted channel for establishment of TLS proxy connections, list of services for which the TSF is able to initiate communications. There is no change to the Base-PP EAs for this

SFR when this PP-Module is claimed.

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1
There is no change to the Base-PP EAs for this SFR when this PP-Module is claimed.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_GCR_EXT.1 Generation of Certificate Repository

FAU_GCR_EXT.1
TSS
Guidance
Tests

FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4
TSS
Guidance
Tests

2.2.2 Cryptographic Support (FCS)

FCS_COP.1/STIP Cryptographic Operation (Data Encryption/Decryption in Support of STIP

FCS_COP.1/STIP
TSS
Guidance
Tests

FCS_STG_EXT.1 Cryptographic Key Storage

FCS_STG_EXT.1
TSS
Guidance
Tests

FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTC_EXT.1.1
TSS

Guidance

Tests

FCS_TTTC_EXT.1.2
TSS

Guidance

Tests

FCS_TTTC_EXT.1.3
TSS

Guidance

Tests

FCS_TTTC_EXT.1.4
TSS

Guidance

Tests

FCS_TTTC_EXT.5 Thru-Traffic TLS Inspection Client Support for Supported Groups Extension

FCS_TTTC_EXT.5
TSS
Guidance
Tests

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FCS_TTTS_EXT.1.1
TSS

Guidance

Tests

FCS_TTTS_EXT.1.2
TSS

Guidance

Tests

FCS_TTTS_EXT.1.3
TSS

Guidance

Tests

2.2.3 User Data Protection (FDP)

FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.1
TSS
Guidance
Tests

FDP_CER_EXT.2 Certificate Request Matching of Server Certificates

FDP_CER_EXT.2
TSS
Guidance
Tests

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

FDP_CER_EXT.3
TSS
Guidance
Tests

FDP_CSIR_EXT.1 Certificate Status Information Required

FDP_CSIR_EXT.1
TSS
Guidance
Tests

FDP_PPP_EXT.1 Plaintext Processing Policy

FDP_PPP_EXT.1
TSS
Guidance
Tests

FDP_PRC_EXT.1 Plaintext Routing Control

FDP_PRC_EXT.1
TSS
Guidance
Tests

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1
TSS
Guidance
Tests

FDP_STG_EXT.1 Certificate Data Storage

FDP_STG_EXT.1
TSS
Guidance
Tests

FDP_STIP_EXT.1 SSL/TLS Inspection Proxy Functions

FDP_STIP_EXT.1.1
TSS

Guidance

Tests

FDP_STIP_EXT.1.2
TSS

Guidance

Tests

FDP_STIP_EXT.1.3
TSS

Guidance

Tests

FDP_STIP_EXT.1.4
TSS

Guidance

Tests

FDP_STIP_EXT.1.5
TSS

Guidance

Tests

FDP_TEP_EXT.1 SSL/TLS Inspection Proxy Policy

FDP_TEP_EXT.1
TSS
The evaluator shall examine the TSS and verify that the TLS session establishment policy is adequately described. The evaluator shall verify that the TSS description of the TLS session establishment policy includes a discussion of the TOE’s initialization/startup process, which clearly indicates where processing of TLS messages begins and provides a discussion that supports the assertion that TLS messages are dropped during this process.

The evaluator shall verify that the TSS also includes a narrative that identifies the components involved in processing TLS messages and describe the safeguards that would prevent inspection or Bypass Operation functions being performed in the event of a component failure. This could include the failure of a component

or a failure within a component. The evaluator shall also verity that the TSS description indicates how the TLS protocol is recognized at each client side and server side interface.

The evaluator shall examine the TSS and verify that it describes any non-configurable rules implementing the TLS session establishment policy and that it describes how such rules invoke the inspect, bypass, or block operations based on the subject attributes included in FDP_TEP_EXT.1.2.

The evaluator shall verify that the TSS describes a TLS session establishment policy and the attributes identified in FDP_TEP_EXT.1.2 are identified as being configurable within the TLS session establishment policy rules. The evaluator shall verify that each configurable rule of the TLS session establishment policy can identify the block, bypass or inspect operation, with the option to log block and bypass operation.

The evaluator shall examine the TSS and verify that rules to define server allowances, client allowances, and other entity allowances (if supported) for TLS parameter usage and TLS processing errors that depend on the TLS session establishment policy is described and includes all conditions indicated in FDP_TEP_EXT.1.5. If multiple response options for receiving a client certificate request message from a requested server are selected in FDP_TEP_EXT.1.7, the evaluator shall confirm that the ‘mutual authentication block-bypass’ specification is claimed in FDP_TEP_EXT.1.5 and that a description of the processing rules for a TLS client certificate request are included in the TSS description of the TLS session establishment policy.

If mutual authentication for through-traffic processing is supported, the evaluator shall examine the TSS and verify that policy rules to define when mutual authentication is allowed are described.

The evaluator shall examine the TSS and verify that description of the TLS protocol and TLS session establishment policy describe the policy-specified behavior that results from TLS protocol errors as required in FDP_TEP_EXT.1.8.

The evaluator shall examine the TSS and verify that the default rules indicated in FDP_TEP_EXT.1.9 and FDP_TEP_EXT.1.10 are described.

Guidance

The evaluator shall examine the operational guidance to verify that instructions to configure the TLS session establishment policy are provided.

The evaluator shall examine the AGD guidance documents and verify that they identify all attributes included in FDP_TEP_EXT.1.2 as being configurable within the TLS session establishment policy, which is that all configurable features of the TLS session establishment policy function are described in the operational guidance.

The evaluator shall examine the AGD guidance documents and verify they indicate each rule can identify the following operations: block, bypass, and inspect. The evaluator shall confirm that instructions for configuring the inspection, bypass, and block operations within rules are included.

The evaluator shall examine the AGD guidance documents and verify they specify each rule indicating block or bypass operations can designate whether logging or counting of TLS Client Hello messages invoking the operation is performed.

The evaluator shall examine the AGD guidance documents and verify they provide instructions on configuring the TLS parameter allowances identified in FDP_TEP_EXT.1.5 and those responses to TLS protocol errors identified in FDP_TEP_EXT.1.8.are indicated.

The evaluator shall examine the AGD guidance documents and verify that any instructions required to configure the TLS session establishment policy to meet the requirements in this component are provided.

Tests

Setup: The evaluator shall configure one or more monitored clients to present TLS requests to various TLS servers through the TOE. The TLS servers will obtain certificates issued by an external certification authority trusted by the TSF. The client, server, and the server certificates will meet the conditions described in each test. The evaluator shall configure the TOE according to operational guidance to have non-trivial rules for all TLS session establishment policy states. The evaluator shall conduct the following tests, establishing any additional configuration requirements as indicated in each.

- **Test 1:** For each rule of the TLS establishment policy indicating inspection operation processing, the evaluator shall ensure the monitored client is configured to meet the requirements for FCS_TLSC_EXT.1, the requested server is configured to meet the requirements for FCS_TLSS_EXT.1, and the server certificate is valid according to FIA_X509_EXT.1/STIP. The evaluator shall configure the TSF so the rule applies to the monitored client and requested server. The evaluator shall establish a TLS session from the monitored client to the requested server through the TOE. The evaluator shall then observe the TSF audit record, certificate repository, TLS Server Hello data received at the client, plaintext encrypted at the client, and plaintext decrypted by the requested server. The evaluator shall then confirm that the TSF established a TLS session with the requested server, issued a certificate representing the requested server, established a TLS session with the monitored client, decrypted the data, performed any inspection processing, and presented the data to the requested server via the established TLS session.
- **Test 2:** For each rule of the TLS establishment policy indicating bypass processing, the evaluator shall establish a monitored client, requested server, and server certificate that meets the rule. The evaluator shall send a TLS request from the monitored client to the requested server through the TOE, and then inspect logs, certificate repository, certificate received by the monitored client in the Server Hello message, plaintext encrypted by the monitored client, and plaintext decrypted by the requested server to

confirm that bypass processing occurred.

- **Test 3:** The evaluator shall follow AGD guidance to ensure the TSF is configured to log blocked TLS sessions. For each rule of the TLS establishment policy indicating blocking of the TLS session, as indicated in any element of this component, the evaluator shall establish that a monitored client, a requested server, and a server certificate meet the rule. The evaluator shall send a TLS session from the monitored client to the requested server through the TOE and observe that the monitored client receives an error response in accordance with FDP_STIP_EXT.1.5 indicating that the session was blocked. The evaluator shall inspect the TSF logs to verify that each session was recorded as blocked.
- **Test 4:** For each event that initiates a transition from the inspection operation to the block operation, the evaluator shall attempt to establish a monitored client and requested server, and configure the TOE and its TLS session establishment policy to invoke the event. For each such event, the evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE. The evaluator shall monitor traffic between the monitored client and the TOE, and monitor traffic between the TOE and the requested client, observing that TLS handshake messages prior to the event are sent, and that any TLS sessions established prior to the event are terminated on transition of the session to the block operation. The evaluator shall observe that the monitored client receives the specified error message indicating that the TLS session is blocked.
- **Test 5:** Test 5 [conditional, both 'mutual authentication inspection' and 'send an empty certificate list as part of the inspection operation' are selected in FDP_TEP_EXT.1.7]: The evaluator shall establish a server to send certificate requests in its TLS handshake. The evaluator shall extablish a monitored client configured to provide a valid client certificate in response to a certificate request. The evaluator shall follow AGD guidance to configure the TLS inspection proxy policy to send an empty certificate list in a certificate message to the server, and initiate a TLS request from a monitored client to the server through the TOE. The evaluator shall observe network traffic between the TOE and the requested server and confirm that the TOE sends an empty certificate list to the server after receiving the certificate request.

  Using the same server, the evaluator shall follow AGD guidance to configure the TSF to perform mutual authentication inspection with the server, and initiate a TLS request from the same monitored client ro the same requested server through the TOE. The evaluator shall observe network traffic between the TOE and the requested server and confirm the TOE sends a certificate message containing a client certificate representing the monitored client.

2.2.4 Identification and Authentication (FIA)

FIA_ENR_EXT.1 Certificate Enrollment

FIA_ENR_EXT.1
TSS
Guidance
Tests

FIA_X509_EXT.1/STIP X.509 Certificate Validation (STIP)

FIA_X509_EXT.1/STIP
TSS
Guidance
Tests

2.2.5 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1
TSS
Guidance
Tests

FPT_KST_EXT.1 No Plaintext Key Export

FPT_KST_EXT.1
TSS
Guidance
Tests

FPT_KST_EXT.2 TSF Key Protection

FPT_KST_EXT.2
TSS
Guidance
Tests

FPT_RCV.1 Manual Trusted Recovery

FPT_RCV.1
TSS
Guidance
Tests

2.3 Evaluation Activities for Optional SFRs

2.3.1 Persistent Local Audit Storage

FAU_SAR.1 Audit Review

FAU_SAR.1
TSS
Guidance
Tests

FAU_SAR.3 Selectable Audit Review

FAU_SAR.3
TSS
Guidance
Tests

2.3.2 Certificate Pinning

FDP_PIN_EXT.1 Certificate Pinning

FDP_PIN_EXT.1
TSS
Guidance
Tests

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Certificate Status Information

FDP_CRL_EXT.1 Certificate Revocation List Generation

FDP_CRL_EXT.1
TSS
Guidance
Tests

FDP_CSI_EXT.1 Certificate Status Information

FDP_CSI_EXT.1
TSS
Guidance
Tests

FDP_OCSP_EXT.1 OCSP Basic Response Generation

FDP_OCSP_EXT.1
TSS
Guidance
Tests

FCS_OCSPS_EXT.1 OCSP Stapling

FCS_OCSPS_EXT.1
TSS
Guidance
Tests

2.4.2 Certificate Enrollment

FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client

FIA_ESTC_EXT.1
TSS
Guidance
Tests

2.4.3 Inspection Policy Banner

FTA_TAB.1/TLS TOE Access Banner (Consent to Monitor Banner for TLS Inspection

FTA_TAB.1/TLS
TSS
Guidance
Tests

2.4.4 Authentication of Monitored Clients

FCS_TTTC_EXT.3 Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients

FCS_TTTC_EXT.3
TSS
Guidance
Tests

FCS_TTTS_EXT.3 Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients

FCS_TTTS_EXT.3
TSS
Guidance
Tests

FDP_CER_EXT.4 Certificate Profiles for Client Certificates

FDP_CER_EXT.4
TSS
Guidance
Tests

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

FDP_CER_EXT.5
TSS
Guidance
Tests

FDP_CSI_EXT.2 Certificate Status Information for Client Certificates

FDP_CSI_EXT.2
TSS
Guidance
Tests

FDP_STIP_EXT.2 Mutual Authentication Inspection Operation

FDP_STIP_EXT.2
TSS
Guidance
Tests

2.4.5 Other Selection-Based SFRs

FAU_SCR_EXT.1 Certificate Repository Review

FAU_SCR_EXT.1
TSS
Guidance

Tests

FCS_CKM_EXT.5 Public Key Integrity

FCS_CKM_EXT.5
TSS
Guidance
Tests

FCS_TTTC_EXT.4 STIP Client-Side Support for Renegotiation

FCS_TTTC_EXT.4
TSS
Guidance
Tests
FCS_TTTC_EXT.4.3
TSS

Guidance

Tests

FCS_TTTS_EXT.4 STIP Server-Side Support for Renegotiation

FCS_TTTS_EXT.4
TSS
Guidance
Tests

2.4.6 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS
The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based preshared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported. The evaluator shall also confirm that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the FIA_PSK_EXT.1.3.

Guidance
If the TOE supports bit-based pre-shared keys, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre- shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

The evaluator shall check that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.

The evaluator shall examine the operational guidance to determine that it provides guidance on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must include, at minimum, the same items contained in FIA_PSK_EXT.1.2.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.
- **Test 2:** [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and invalid lengths that are below the minimum length, above the maximum length, null length, empty length, or zero length. The minimum and maximum length tests should be successful, and the invalid lengths must be rejected by the TOE.
- **Test 3:** [conditional]: If the TOE supports but does not generate bit-based pre-shared keys, the evaluator

shall obtain a bit-based pre-shared key of the appropriate length and enter it per the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

- **Test 4:** [conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base General Purpose Operating Systems PP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The General Purpose Operating Systems PP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[OS PP]	Protection Profile for General Purpose Operating Systems, Version 4.2.1, April 2019
[MD PP]	Protection Profile for Mobile Device Fundamentals, Version 3.1, June 2017
[MDM PP]	Protection Profile for Mobile Device Management (This needs to be updated) , Version 3.1, June 2017
[App PP]	Protection Profile for Application Software, Version 1.3, March 2019
[SD]	Supporting Document Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, November 2019