Supporting Document
Mandatory Technical Document

PP-Module for VPN Client
Version: 2.6
2025-01-31
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
2.6	2025-01-31	CC:2022 conversion, limitation of cryptographic algorithms to CNSA 1.0, incorporation of TDs
2.5	2024-06-24	Incorporation of TC feedback: • Incorporation of TDs: 0662, 0672, 0690, 0697, 0711, 0725, 0753, 0788 • Corrections to Base-PP references • Definition of auditable events for Additional SFRs • Explicit association of evaluation activities with components and elements
2.4	2022-03-31	Incorporation of TC feedback

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of VPN client products.

Acknowledgments:
This SD was developed with support from NIAP VPN client 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 VPN Client is to describe the security functionality of VPN client 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-PPs:

- Protection Profile for General Purpose Operating System, version 4.3.
- Protection Profile for Mobile Device Fundamentals, version 3.3.
- Protection Profile for Application Software, version 1.4.
- Protection Profile for Mobile Device Management, version 4.0.

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

- VPN client, Version 2.6

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities 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.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
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.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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-PPs.
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.
Target of Evaluation (TOE)	The product under evaluation.
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.

1.3.2 Technical Terms

Administrator	A user that has administrative privilege to configure the TOE in privileged mode.
Authorized	An entity granted access privileges to an object, system, or system entity.
Critical Security Parameter (CSP)	Security related information such as secret and private cryptographic keys, and authentication data such as passwords and PINs, whose disclosure or modification can compromise the security of a cryptographic module.
Entropy Source	This cryptographic function provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.
IT Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Private Network	A network that is protected from access by unauthorized users or entities.
Privileged Mode	A TOE operational mode that allows a user to perform functions that require IT environment administrator privileges.
Public Network	A network that is visible to all users and entities and does not protect against unauthorized access (e.g. internet).
Threat Agent	An entity that tries to harm an information system through destruction, disclosure, modification of data, or denial of service.
Unauthorized User	An entity (device or user) that has not been authorized by an authorized administrator to access the TOE or private network.
Unprivileged Mode	A TOE operational mode that only provides VPN client functions for the VPN client user.
VPN Client	The TOE; allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to a private network.
VPN Client User	A user operating the TOE in unprivileged mode.
VPN Gateway	A component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network.

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 labeled 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 labeled 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 System

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

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the GPOS PP is the base.

2.1.2 Additional SFRs

2.1.2.1 Cryptographic Support (FCS)

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the VPN client or the OS, the evaluator shall check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.

The evaluator shall review the TSS to determine that it makes a case that, for each item listed as being manipulated, it is not written unencrypted to persistent memory, and that the item is stored by the OS.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this component.

2.1.2.2 Identification and Authentication (FIA)

FIA_X509_EXT.4 X.509 Certificate Use and Management

FIA_X509_EXT.4.1
FIA_X509_EXT.4.1 is evaluated as part of FCS_IPSEC_EXT.1 (and conditionally as part of FPT_TUD_EXT.1 or FPT_TST_EXT.1).

FIA_X509_EXT.4.2
TSS
The evaluator shall check the TSS to ensure that it describes whether the VPN client or the OS implements the certificate validation functionality, how the VPN client/OS chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the OS so that desired certificates can be used.

The evaluator shall examine the TSS to confirm that it describes the behavior of the client/OS when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

Guidance
If the requirement indicates that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.

Tests

The evaluator shall perform the following test regardless of whether the certificate validation functionality is implemented by the VPN client or by the OS:

- Test FIA_X509_EXT.4.2:1: 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.4.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.

FIA_X509_EXT.4.3
FIA_X509_EXT.4.3 is evaluated as part of FCS_IPSEC_EXT.1.11.

2.1.2.3 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1
TSS
The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN gateway, VPN client, or IPsec-capable network device in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Guidance
The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to a VPN gateway, VPN client, or IPsec-capable network device, and that it contains recovery instructions should a connection be unintentionally broken.

Tests
The evaluator shall perform the following tests:

- Test FTP_ITC.1:1: The evaluator shall ensure that the TOE is able to initiate communications with a VPN gateway, VPN client, or IPsec-capable network device using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful.
- Test FTP_ITC.1:2: The evaluator shall ensure, for each communication channel with an IPsec peer, the channel data is not sent in plaintext.
- Test FTP_ITC.1:3: The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE.
- Test FTP_ITC.1:4: The evaluator shall physically interrupt the connection from the TOE to the IPsec peer. The evaluator shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.

Further EAs are associated with requirements for FCS_IPSEC_EXT.1.

2.2 Protection Profile for Mobile Device Fundamentals

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

2.2.1 Modified SFRs

The PP-Module does not modify any requirements when the MDF PP is the base.

2.2.2 Additional SFRs

2.2.2.1 User Data Protection (FDP)

FDP_VPN_EXT.1 Split Tunnel Prevention

FDP_VPN_EXT.1.1
TSS
The evaluator shall verify that the TSS section of the ST describes the routing of IP traffic through processes on the TSF when a VPN client is enabled. The evaluator shall ensure that the description indicates which traffic does not go through the VPN and which traffic does and that a configuration exists for each baseband protocol in which only the traffic identified by the ST author is necessary for establishing the VPN connection (IKE traffic and perhaps HTTPS or DNS traffic) is not encapsulated by the VPN protocol (IPsec). The ST author shall also identify in the TSS section any differences in the routing of IP traffic when using any supported baseband protocols (e.g. Wi-Fi, LTE).

Guidance
The evaluator shall verify that the following is addressed by the documentation:

- The description above indicates that if a VPN client is enabled, all configurations route all IP traffic (other than IP traffic required to establish the VPN connection) through the VPN client.
- The guidance describes how the user or administrator can configure the TSF to meet this requirement.

Tests
The evaluator shall perform the following test:

Step 1 - The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an internet-connected network. The evaluator shall turn on the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data.

Step 2 - The evaluator shall configure an IPsec VPN client that supports the routing specified in this requirement, and if necessary, configure the device to perform the routing specified as described in the AGD guidance. The evaluator shall turn on the sniffing tool, establish the VPN connection, and perform the same actions with the device as performed in the first step. The evaluator shall verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data.

Step 3 - The evaluator shall examine the traffic from both step one and step two to verify that all IP traffic, aside from and after traffic necessary for establishing the VPN (such as IKE, DNS, and possibly HTTPS), is encapsulated by IPsec.

Step 4 - The evaluator shall attempt to send packets to the TOE outside the VPN connection and shall verify that the TOE discards them.

2.3 Protection Profile for Application Software

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

2.3.1 Modified SFRs

The PP-Module does not modify any requirements when the App PP is the base.

2.3.2 Additional SFRs

2.3.2.1 Cryptographic Support (FCS)

FCS_CKM.6 Cryptographic Key Destruction

FCS_CKM.6
TSS
The evaluator shall ensure that all plaintext secret and private cryptographic keys and CSPs (whether manipulated by the TOE or exclusively by the platform) are identified in the VPN client ST's TSS, and that they are accounted for by the EAs in this section.

Requirement met by the platform:

The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and CSPs used to generate keys that are not otherwise covered by the FCS_CKM.6 requirement levied on the TOE.

For each platform listed in the ST, the evaluator shall examine the TSS of the ST of the platform to ensure that each of the secret keys, private keys, and CSPs used to generate the keys listed above are covered.

Requirement met by the TOE:

The evaluator shall check to ensure the TSS describes when each of the plaintext keys are cleared (e.g., system power off, disconnection of an IPsec connection, when no longer needed by the VPN channel per the protocol); and the type of clearing procedure that is performed (cryptographic erase, overwrite with zeros, overwrite three or more times by a different alternating pattern, overwrite with random pattern, or block erase). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting three times with a random pattern that is changed before each write").

Guidance
There are no guidance EAs for this requirement.

Tests
For each key clearing situation described in the TSS, the evaluator shall repeat the following test.

- Test FCS_CKM.6:1: The evaluator shall use appropriate combinations of specialized OE and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

  Cryptographic TOE implementations in software shall be loaded and exercised under a debugger to perform such tests. The evaluator shall perform the following test for each key subject to clearing, including intermediate copies of keys that are persisted encrypted by the TOE:

  1. Load the instrumented TOE build in a debugger.
  2. Record the value of the key in the TOE subject to clearing.
  3. Cause the TOE to perform a normal cryptographic processing with the key from #1.
  4. Cause the TOE to clear the key.
  5. Cause the TOE to stop the execution but not exit.
  6. Cause the TOE to dump the entire memory footprint of the TOE into a binary file.
  7. Search the content of the binary file created in #6 for instances of the known key value from #1.

  The test succeeds if no copies of the key from #1 are found in step #7 above and fails otherwise.

  The evaluator shall perform this test on all keys, including those persisted in encrypted form, to ensure intermediate copies are cleared.

FCS_CKM_EXT.2 Cryptographic Key Storage

FCS_CKM_EXT.2.1
TSS
Regardless of whether this requirement is met by the TOE or the TOE platform, the evaluator shall check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored. The evaluator shall then perform the following actions:

Persistent secrets and private keys manipulated by the platform:

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the persistent secrets and private keys listed as being stored by the platform in the VPN client ST are identified as being protected in that platform's ST

Persistent secrets and private keys manipulated by the TOE:

The evaluator shall review the TSS to determine that it makes a case that, for each item listed as being manipulated by the TOE, it is not written unencrypted to persistent memory, and that the item is stored by the platform.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this requirement.

2.4 Protection Profile for Mobile Device Management

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

2.4.1 Modified SFRs

The PP-Module does not modify any requirements when the MDM PP is the base.

2.5 TOE SFR Evaluation Activities

2.5.1 Cryptographic Support (FCS)

FCS_CKM.1/VPN VPN Cryptographic Key Generation (IKE)

FCS_CKM.1.1/VPN
TSS
The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.

Guidance
There are no guidance EAs for this requirement.

Tests
If this functionality is implemented by the TSF, refer to the following EAs, depending on the TOE's claimed Base-PP:

- GPOS PP: FCS_CKM.1
- MDF PP: FCS_CKM.1
- App PP: FCS_CKM.1/AK
- MDM PP: FCS_CKM.1

FCS_IPSEC_EXT.1 IPsec

FCS_IPSEC_EXT.1
TSS
In addition to the TSS EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the TOE boundary includes a general-purpose OS or mobile device, the evaluator shall examine the TSS to ensure that it describes whether the VPN client capability is architecturally integrated with the platform itself or it is a separate executable that is bundled with the platform.

Guidance
In addition to the guidance EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the configuration of the IPsec behavior is from an environmental source, most notably a VPN gateway (e.g through receipt of required connection parameters from a VPN gateway), the evaluator shall ensure that the operational guidance contains any appropriate information for ensuring that this configuration can be properly applied.

Note, in this case, that the implementation of the IPsec protocol must be enforced entirely within the TOE boundary; i.e. it is not permissible for a software application TOE to be a graphical front-end for IPsec functionality implemented totally or in part by the underlying OS platform. The behavior referenced here is for the possibility that the configuration of the IPsec connection is initiated from outside the TOE, which is permissible so long as the TSF is solely responsible for enforcing the configured behavior. However, it is allowable for the TSF to rely on low-level, platform-provided networking functions to implement the SPD from the client (e.g., enforcement of packet routing decisions).

Tests
As a prerequisite for performing the Test EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall do the following:

The evaluator shall minimally create a test environment equivalent to the test environment illustrated below. It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability to manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluator shall provide justification for any differences in the test environment.

Note that the evaluator shall perform all tests using the VPN client and a representative sample of platforms listed in the ST (for TOEs that claim to support multiple platforms).

FCS_IPSEC_EXT.1.1

TSS
The evaluator shall examine the TSS and determine that it describes how the IPsec capabilities are implemented.

If the TOE is a standalone software application, the evaluator shall ensure that the TSS asserts that all IPsec functionality is implemented by the TSF. The evaluator shall also ensure that the TSS identifies what platform functionality the TSF relies on to support its IPsec implementation, if any (e.g. does it invoke cryptographic primitive functions from the platform's cryptographic library, enforcement of packet routing decisions by low-level network drivers).

If the TOE is part of a general-purpose desktop or mobile OS, the evaluator shall ensure that the TSS describes at a high level the architectural relationship between the VPN client portion of the TOE and the rest of the TOE (e.g. is the VPN client an integrated part of the OS or is it a standalone executable that is bundled into the OS package). If the SPD is implemented by the underlying platform in this case, then the TSS describes how the client interacts with the platform to establish and populate the SPD, including the identification of the platform's interfaces that are used by the client.

In all cases, the evaluator shall also ensure that the TSS describes how the client interacts with the network stack of the platforms on which it can run (e.g., does the client insert itself within the stack via kernel mods, does the client simply invoke APIs to gain access to network services).

The evaluator shall ensure that the TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how the available rules and actions form the SPD using terms defined in RFC 4301, such as BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet).

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial, and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Guidance
The evaluator shall examine the operational guidance to verify it describes how the SPD is created and configured. If there is an administrative interface to the client, then the guidance describes how the administrator specifies rules for processing a packet. The description includes all three cases - a rule that ensures packets are encrypted/decrypted, dropped, and allowing a packet to flow in plaintext. The evaluator shall determine that the description in the operational guidance is consistent with the description in the TSS, and that the level of detail in the operational guidance is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

If the client is configured by an external application, such as the VPN gateway, then the operational guidance should indicate this and provide a description of how the client is configured by the external application. The description should contain information as to how the SPD is established and set up in an unambiguous fashion. The description should also include what is configurable via the external application, how ordering of entries may be expressed, as well as the impacts that ordering of entries may have on the packet processing.

In either case, the evaluator shall ensure the description provided in the TSS is consistent with the capabilities and description provided in the operational guidance.

Tests
Depending on the implementation, the evaluator may be required to use a VPN gateway or some form of application to configure the client. For Test 2, the evaluator is required to choose an application that allows for the configuration of the full set of capabilities of the VPN client (in conjunction with the platform). For example, if the client provides a robust interface that allows for specification of wildcards, subnets, etc., it is unacceptable for the evaluator to choose a VPN gateway that only allows for specifying a single fully qualified IP addresses in the rule.

The evaluator shall perform the following tests:

- Test FCS_IPSEC_EXT.1.1:1: The evaluator shall configure an SPD on the client that is capable of the following: dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the client with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator shall perform both positive and negative test cases for each type of rule. The evaluator shall observe via the audit trail and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed through without modification, was encrypted by the IPsec implementation.
- Test FCS_IPSEC_EXT.1.1:2: The evaluator shall devise several tests that cover a variety of scenarios for

packet processing. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and operational guidance. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the operational guidance.

FCS_IPSEC_EXT.1.2
TSS
The evaluator shall check the TSS to ensure it states that the VPN can be established to operate in tunnel mode, transport mode, or both (as selected).

Guidance
The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

If both transport and tunnel modes are implemented, the evaluator shall review the operational guidance to determine how the use of a given mode is specified.

Tests
The evaluator shall perform the following tests based on the selections chosen:

- Test FCS_IPSEC_EXT.1.2:1: [conditional]: If tunnel mode is selected, the evaluator shall use the operational guidance to configure the TOE and a VPN gateway to operate in tunnel mode. The evaluator shall configure the TOE and the VPN gateway to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the VPN gateway peer. The evaluator shall observe (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
- Test FCS_IPSEC_EXT.1.2:2: [conditional]: If transport mode is selected, the evaluator shall use the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec peer to accept IPsec connections using transport mode. The evaluator shall configure the TOE and the endpoint device to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE to connect to the remote endpoint. The evaluator shall observe (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.
- Test FCS_IPSEC_EXT.1.2:3: [conditional]: If both tunnel and transport modes are selected, the evaluator shall perform both Test 1 and Test 2 above, demonstrating that the TOE can be configured to support both modes.
- Test FCS_IPSEC_EXT.1.2:4: [conditional]: If both tunnel and transport modes are selected, the evaluator shall modify the testing for FCS_IPSEC_EXT.1 to include the supported mode for SPD PROTECT entries to show that they only apply to traffic that is transmitted or received using the indicated mode.

FCS_IPSEC_EXT.1.3
TSS
The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Guidance
The evaluator shall check that the operational guidance provides instructions on how to construct or acquire the SPD and uses the guidance to configure the TOE for the following test.

Tests
The evaluator shall perform the following test:

- Test FCS_IPSEC_EXT.1.3:1: The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, PROTECT, and (if applicable) BYPASS network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a “TOE-created” final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE’s interfaces.

FCS_IPSEC_EXT.1.4
TSS
The evaluator shall examine the TSS to verify that the algorithm AES-GCM-256 is implemented. If the ST author has selected AES-CBC-256 in the requirement, then the evaluator shall verify that the TSS describes this as well. In addition, the evaluator shall ensure that the SHA-based HMAC algorithm conforms to the algorithms specified in the relevant iteration of FCS_COP.1 from the Base-PP that applies to keyed-hash message authentication.

Guidance
The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.

Tests

- Test FCS_IPSEC_EXT.1.4:1: The evaluator shall configure the TOE as indicated in the operational guidance, configuring the TOE to using the AES-GCM-256 algorithm, and attempt to establish a connection using ESP. If the ST author has selected AES-CBC-256, the TOE is configured to use this algorithm, and the evaluator shall attempt to establish a connection using ESP for those algorithms selected.

FCS_IPSEC_EXT.1.5
TSS
The evaluator shall examine the TSS to verify that IKEv1, IKEv2, or both are implemented. If IKEv1 is implemented, the evaluator shall verify that the TSS indicates whether XAUTH is supported, and that aggressive mode is not used for IKEv1 Phase 1 exchanges (i.e. only main mode is used). It may be that these are configurable options.

Guidance
The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1, IKEv2, or both (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the tests below. If XAUTH is implemented, the evaluator shall verify that the operational guidance provides instructions on how it is enabled or disabled.

If the TOE supports IKEv1, the evaluator shall verify that the operational guidance either asserts that only main mode is used for Phase 1 exchanges or provides instructions for disabling aggressive mode.

Tests

- Test FCS_IPSEC_EXT.1.5:1: The evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 7296, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed. If the TOE supports IKEv1 with or without XAUTH, the evaluator shall verify that this test can be successfully repeated with XAUTH enabled and disabled in the manner specified by the operational guidance. If the TOE only supports IKEv1 with XAUTH, the evaluator shall verify that connections not using XAUTH are unsuccessful. If the TOE only supports IKEv1 without XAUTH, the evaluator shall verify that connections using XAUTH are unsuccessful.

  In the case that the VPN gateway enforces the TOE's configuration, the following steps shall be performed to meet the objective of Test 1:
  1. Configure the TOE client and VPN gateway to have XAUTH enabled.
  2. Attempt the connection and observe that the connection succeeds and that XAUTH is used.
  3. Configure the TOE and gateway to have XAUTH disabled.
  4. Attempt the connection and observe that the connection succeeds and that XAUTH is not present.
  5. Attempt to configure a mismatch between the TOE and gateway (i.e. modify a local configuration setting on the client system)
  6. Verify that no IPsec connection is attempted until the gateway corrects the configuration settings
- Test FCS_IPSEC_EXT.1.5:2: [conditional]: If the TOE supports IKEv1, the evaluator shall perform any applicable operational guidance steps to disable the use of aggressive mode and then attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator shall show that the TOE will reject a VPN gateway from initiating an IKEv1 Phase 1 connection in aggressive mode. The evaluator should then show that main mode exchanges are supported.

  In the case that the VPN gateway enforces the TOE's configuration, the following steps should be performed to meet the objective of Test 2:
  1. Configure the gateway and TOE client in the appropriate manner per the guidance documentation (i.e., gateway rejects aggressive mode, client rejects aggressive mode).
  2. Connect the TOE client to the gateway to obtain the configuration settings.
  3. Observe the main mode connection is successful.
  4. Disconnect the TOE from the gateway.
  5. Attempt to modify the setting for main mode locally on the TOE to force the client to attempt to use aggressive mode.
  6. Observe that when the initial connection attempt to the gateway is made, the gateway detects the configuration difference and reapplies the main mode setting before the TOE can attempt an IPsec connection.
  7. Configure a peer to have equivalent settings to the VPN gateway (Same ciphers/Authentication/Hash/KEX settings)
  8. Tell the TOE that there is a VPN gateway at the location of the peer.
  9. Observe that the TOE cannot establish a connection with the peer.

FCS_IPSEC_EXT.1.6

TSS
The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKE payload for each supported IKE version and that the algorithm AES-CBC-256 is specified, and if AES-GCM-256 is chosen in the selection of the requirement, this is included in the TSS discussion.

Guidance
The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.

Tests
The evaluator shall use the operational guidance to configure the TOE (or to configure the OE to have the TOE receive configuration) to perform the following test for each ciphersuite selected:

- Test FCS_IPSEC_EXT.1.6:1: The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKE payload for each supported IKE version and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator shall confirm the algorithm was that used in the negotiation. The evaluator shall confirm that the connection is successful by confirming that data can be passed through the connection once it is established. For example, the evaluator may connect to a webpage on the remote network and verify that it can be reached.

FCS_IPSEC_EXT.1.7
TSS
There are no TSS EAs for this requirement.

Guidance
The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE configures the values for SA lifetimes. In addition, the evaluator shall check that the guidance has the option for either the administrator or VPN gateway to configure Phase 1 SAs if time-based limits are supported. Currently, there are no values mandated for the number of packets or number of bytes; the evaluator shall simply check the operational guidance to ensure that this can be configured if selected in the requirement.

Tests
When testing this functionality, the evaluator shall ensure that both sides are configured appropriately. From the RFC “A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered.”

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

- Test FCS_IPSEC_EXT.1.7:1: [conditional]: The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.
- Test FCS_IPSEC_EXT.1.7:2: [conditional]: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.
- Test FCS_IPSEC_EXT.1.7:3: [conditional]: The evaluator shall perform a test similar to Test 2 for Phase 2 SAs, except that the lifetime will be 8 hours or less instead of 24 hours or less.
- Test FCS_IPSEC_EXT.1.7:4: [conditional]: If a fixed limit for IKEv1 SAs is supported, the evaluator shall establish an SA and observe that the connection is closed after the fixed traffic or time value is reached.

FCS_IPSEC_EXT.1.8
TSS
The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator shall check to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

Guidance
There are no guidance EAs for this requirement.

Tests
The evaluator shall perform the following test:

- Test FCS_IPSEC_EXT.1.8:1: For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.

FCS_IPSEC_EXT.1.9
TSS
The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x" (as defined in FCS_IPSEC_EXT.1.9) and each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this EP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this requirement.
FCS_IPSEC_EXT.1.10
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.9.

FCS_IPSEC_EXT.1.11
TSS
The evaluator shall ensure that the TSS describes whether peer authentication is performed using RSA, ECDSA, or both.

If any selection with pre-shared keys is chosen in the selection, the evaluator shall check to ensure that the TSS describes how those selections work in conjunction with authentication of IPsec connections.

The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include whether the certificate presented identifier is compared to the ID payload presented identifier, which fields of the certificate are used as the presented identifier (DN, Common Name, or SAN), and if multiple fields are supported, the logical order comparison. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate.

Guidance
If any selection with "Pre-shared Keys" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.

If any method other than no other method is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.

The evaluator shall ensure that the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA, ECDSA, or either, depending on which is claimed in the ST.

In order to construct the environment and configure the TOE for the following tests, the evaluator shall ensure that the operational guidance also describes how to configure the TOE to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE as a trusted CA.

The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifiers for the peer.

Tests
For efficiency's sake, the testing that is performed here has been combined with the testing for FIA_X509_EXT.2 in Functional Package for X.509, version 1.0 and FIA_X509_EXT.4 (for IPsec connections and depending on the Base-PP), FCS_IPSEC_EXT.1.12 , and FCS_IPSEC_EXT.1.13 . The following tests shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.11 selection above:

For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:
- Test FCS_IPSEC_EXT.1.11:1: The evaluator shall have the TOE generate a public-private key pair and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE a previously generated private key and corresponding certificate.
- Test FCS_IPSEC_EXT.1.11:2: The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.
- Test FCS_IPSEC_EXT.1.11:3: 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 is performed for each method. For this current version of the PP-Module, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used and that the SA is established. The evaluator shall then attempt the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE will not establish an SA.
- Test FCS_IPSEC_EXT.1.11:4: [conditional]: For each selection made, the evaluator shall verify factors are required, as indicated in the operational guidance, to establish an IPsec connection with the server.
- Test FCS_IPSEC_EXT.1.11:5: For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the

field in the peer's presented certificate and shall verify that the IKE authentication succeeds.
- Test FCS_IPSEC_EXT.1.11:6: For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.
- Test FCS_IPSEC_EXT.1.11:7: [conditional]: If, according to the TSS, the TOE supports both Common Name and SAN certificate fields and uses the preferred logic outlined in the Application Note, the tests above with the Common Name field shall be performed using peer certificates with no SAN extension. Additionally, the evaluator shall configure the peer's reference identifier on the TOE to not match the SAN in the peer's presented certificate, but to match the Common Name in the peer's presented certificate and verify that the IKE authentication fails.
- Test FCS_IPSEC_EXT.1.11:8: [conditional]: If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds. To demonstrate a bit-wise comparison of the DN, the evaluator shall change a single bit in the DN (preferably, in an Object Identifier (OID) in the DN) and verify that the IKE authentication fails. To demonstrate a comparison of DN values, the evaluator shall change any one of the four DN values and verify that the IKE authentication fails.
- Test FCS_IPSEC_EXT.1.11:9: [conditional]: If the TOE supports both IPv4 and IPv6 and supports IP address identifier types, the evaluator must repeat tests 1 and 2 with both IPv4 address identifiers and IPv6 identifiers. Additionally, the evaluator shall verify that the TOE verifies that the IP header matches the identifiers by setting the presented identifiers and the reference identifier with the same IP address that differs from the actual IP address of the peer in the IP headers and verifying that the IKE authentication fails.
- Test FCS_IPSEC_EXT.1.11:10: [conditional]: If, according to the TSS, the TOE performs comparisons between the peer's ID payload and the peer's certificate, the evaluator shall repeat the following test for each combination of supported identifier types and supported certificate fields (as above). The evaluator shall configure the peer to present a different ID payload than the field in the peer's presented certificate and verify that the TOE fails to authenticate the IKE peer.

FCS_IPSEC_EXT.1.12
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.

FCS_IPSEC_EXT.1.13
EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.

FCS_IPSEC_EXT.1.14
TSS
The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 or IKEv2 CHILD_SA suites (depending on the supported IKE versions) to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA that is protecting the negotiation.

Guidance
There are no guidance EAs for this requirement.

Tests
The evaluator shall follow the guidance to configure the TOE to perform the following tests:

- Test FCS_IPSEC_EXT.1.14:1: This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
- Test FCS_IPSEC_EXT.1.14:2: [conditional]: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
- Test FCS_IPSEC_EXT.1.14:3: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
- Test FCS_IPSEC_EXT.1.14:4: This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.

2.5.2 User Data Protection (FDP)

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1
TSS
Requirement met by the platform

The evaluator shall examine the TSS to verify that it describes (for each supported platform) the extent to

which the client processes network packets and addresses the FDP_RIP.2 requirement.

Requirement met by the TOE

“Resources” in the context of this requirement are network packets being sent through (as opposed to “to”, as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is reused, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten and at what point in the buffer processing this occurs.

Guidance
There are no guidance EAs for this requirement.

Tests
There are no test EAs for this requirement.

2.5.3 Security Management (FMT)

FMT_SMF.1/VPN Specification of Management Functions (VPN)

FMT_SMF.1.1/VPN
TSS
The evaluator shall check to ensure the TSS describes the client credentials and how they are used by the TOE.

Guidance
The evaluator shall check to make sure that every management function mandated in the ST for this requirement is described in the operational guidance and that the description contains the information required to perform the management duties associated with each management function.

Tests
The evaluator shall test the TOE’s ability to provide the management functions by configuring the TOE according to the operational guidance and testing of each management activity listed in the ST.

The evaluator shall ensure that all management functions claimed in the ST can be performed by completing activities described in the AGD. Note that this may be performed in the course of completing other testing.

2.5.4 Protection of the TSF (FPT)

FPT_TST_EXT.1/VPN TSF Self-Test

FPT_TST_EXT.1/VPN
TSS
The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on startup; 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. If some of the tests are performed by the TOE platform, the evaluator shall check the TSS to ensure that those tests are identified and that the ST for each platform contains a description of those tests. Note that the tests that are required by this component are those that support security functionality in this PP-Module, which may not correspond to the set of all self-tests contained in the platform STs.

The evaluator shall examine the TSS to ensure that it describes how the integrity of stored TSF executable code is cryptographically verified when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator shall check to ensure that the cryptographic requirements listed are consistent with the description of the integrity verification process.

Guidance
If not present in the TSS, the evaluator shall ensure that the operational guidance describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. For checks implemented entirely by the platform, the evaluator shall ensure that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

Tests
The evaluator shall perform the following tests:

- Test FPT_TST_EXT.1/VPN:1: The evaluator shall perform the integrity check on a known good TSF executable and verifies that the check is successful.
- Test FPT_TST_EXT.1/VPN:2: The evaluator shall modify the TSF executable, performs the integrity check on the modified TSF executable, and verifies that the check fails.

2.6 Evaluation Activities for Optional SFRs

2.6.1 Identification and Authentication (FIA)

FIA_BMA_EXT.1 Biometric Activation

FIA_BMA_EXT.1.1
TSS
The evaluator shall confirm that the TSS describes the calls to the platform and verifies they align with platform documentation.

Guidance
The evaluator shall ensure that any configuration details needed to enable the biometric prompt are included in the guidance documentation.

Tests

- Test FIA_BMA_EXT.1.1:1: The evaluator shall initiate a connection and verify that a biometric prompt is presented and accepted before the connection can proceed. The evaluator shall also verify the connection does not proceed if the biometric is not presented or accepted.

2.6.2 Packet Filtering (FPF)

FPF_MFA_EXT.1 Multifactor Authentication Filtering

FPF_MFA_EXT.1.1
TSS
The evaluator shall examine the TSS to verify that it describes how authentication packets are identified and how all other traffic is blocked until secondary authentication is successful.

Guidance
The evaluator shall examine the operational guidance to verify that it provides any necessary instructions to the administrator on how to enable and configure filtering.

Tests

- Test FPF_MFA_EXT.1.1:1: The evaluator shall attempt to connect and verify other traffic is rejected per the filtering rules. The evaluator shall then provide the supported PSKs and confirm it is accepted and traffic is no longer blocked.

2.7 Evaluation Activities for Selection-Based SFRs

2.7.1 Cryptographic Support (FCS)

FCS_EAP_EXT.1 EAP-TLS

FCS_EAP_EXT.1
TSS
The evaluator shall verify that the TSS describes the use of EAP options for each of the selected peer authentication mechanisms, that TLS with mutual authentication is used, that the random values are from an appropriate source, and that the EAP MSK is derived from the TLS master key and is used as the IKEv2 shared key.

Guidance
The evaluator shall verify that the guidance documents describe any configurable features of the EAP or TLS functionality, including instructions for configuration of the authenticators and registration processes for clients.

Tests
Testing for TLS functionality is in accordance with the TLS package. For each supported EAP method claimed in FCS_EAP_TLS_EXT.1.1 and for each authentication method claimed in FCS_EAP_TLS_EXT.1.3, the evaluator shall perform the following tests:

- Test FCS_EAP_EXT.1:1: The evaluator shall follow AGD guidance to configure the TSF to use the EAP method claimed. The evaluator shall follow AGD guidance to configure the TSF to use the authentication method claimed, and for EAP-TTLS, register a client with the appropriate key material required for the authentication method. The evaluator shall establish a VPN session using a test client with a valid certificate, and for EAP-TTLS, configured to provide a correct value for the configured authenticator. The evaluator shall observe the the VPN session is successful.
- Test FCS_EAP_EXT.1:2: (conditional for EAP-TTLS support): The evaluator shall cause the test client with a valid certificate to send an invalid authenticator for the claimed authentication method. For HOTP, replay the HOTP value sent previously. For TOTP or PSK, modify a byte of the properly constructed value and observe that the TSF aborts the session.
- Test FCS_EAP_EXT.1:3: The evaluator shall establish a new, valid certificate for a test client using an identifier not corresponding to a registered user. For EAP-TTLS, the evaluator shall cause the test client using this certificate to send a correct authenticator value for the registered user. The evaluator shall initiate a VPN session from the test client to the TSF and observe that the TSF aborts the session.
- Test FCS_EAP_EXT.1:4: The evaluator shall follow AGD guidance to configure the TSF to use a supported EAP method and register the user with the key material required for a supported authentication method. The evaluator shall configure a test client to respond to an IKEv2 exchange with EAP-request, providing valid phase 1 handshake and valid TLS handshake, but computing the phase 2 shared key using standard (non-EAP) methods. The evaluator shall initiate a VPN session between the test client and the TSF, and observe that the TSF aborts the session.

2.7.2 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it identifies all protocols that allow pre-shared keys. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states which pre-shared key selections are supported.

Guidance
The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required.

The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure the mandatory_or_not flag per RFC 8784.
Tests
The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE).

- Test FIA_PSK_EXT.1:1: For each mechanism selected in FIA_PSK_EXT.1.2, the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection in alignment with table 1 from RFC 8784.

FIA_PSK_EXT.2 Generated Pre-Shared Keys

FIA_PSK_EXT.2.1
TSS
If "generate" is selected, the evaluator shall confirm that this process uses the RBG specified in FCS_RBG.1 (or FCS_RBG_EXT.1 in the case of [App PP] and the output matches the size selected in FIA_PSK_EXT.2.1.

Guidance
The evaluator shall confirm the operational guidance contains instructions for entering generated pre-shared keys for each protocol identified in the FIA_PSK_EXT.1.1.

Tests

- Test FIA_PSK_EXT.2.1:1: [conditional] If "generate" was selected, the evaluator shall generate a pre-shared key and confirm the output matches the size selected in FIA_PSK_EXT.2.1.

FIA_PSK_EXT.3 Password-Based Pre-Shared Keys

FIA_PSK_EXT.3
TSS
The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are used.

Support for length: The evaluator shall check to ensure that the TSS describes the allowable ranges for PSK lengths, and that at least 64 characters or a length defined by the platform may be specified by the user.

Support for character set: The evaluator shall check to ensure that the TSS describes the allowable character set and that it contains the characters listed in the SFR.

Support for PBKDF: The evaluator shall examine the TSS to ensure that the use of PBKDF2 is described and that the key sizes match that described by the ST author.

The evaluator shall check that the TSS describes the method by which the PSK is first encoded and then fed to the hash algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself.

For the NIST SP 800-132-based conditioning of the PSK, the required evaluation activities will be performed when doing the evaluation activities for the appropriate requirements (FCS_COP.1/KeyedHash).

The evaluator shall confirm that the minimum length is described.

The ST author shall provide a description in the TSS regarding the salt generation. The evaluator shall confirm that the salt is generated using an RBG described in the DRBG that is generated by the TSF or that is invoked from the operational environment.

[conditional] If "password strength meter" or "check the password against a denylist" is selected, the evaluator shall examine the TSS to ensure any password checking functionality provided by the TSF is described and contains details on how the function operates.

Guidance
The evaluator shall confirm the operational guidance contains instructions for entering bit-based pre-shared keys for each protocol identified in the requirement, is generating a bit-based pre-shared key, or both. The evaluator shall confirm that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.

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.3.2.

The evaluator shall confirm the operational guidance contains any necessary instructions for enabling and configuring password checking functionality.

Tests
Support for Password/Passphrase characteristics: In addition to the analysis above, the evaluator shall also perform the following tests on a TOE configured according to the operational guidance:

- Test FIA_PSK_EXT.3:1: The evaluator shall compose a pre-shared key of at least 64 characters that contains a combination of the allowed characters in accordance with the FIA_PSK_EXT.1.3 and verify that a successful protocol negotiation can be performed with the key.
- Test FIA_PSK_EXT.3:2: [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length and invalid lengths that are below the minimum length, above the maximum length, null length, empty length, or zero length. The minimum test should be successful, and the invalid lengths must be rejected by the TOE.
- Test FIA_PSK_EXT.3:3: [conditional]: If the TOE initiates connections, initiate and establish a remote connection, disconnect from the connection, and verify that the PSK is required when initiating the connection a second time.
- Test FIA_PSK_EXT.3:4: [conditional]: If the TOE supports a password meter, the evaluator shall enter a password and verify the password checker responds per the description in the TSS.
- Test FIA_PSK_EXT.3:5: [conditional]: If the TOE supports a password denylist, the evaluator shall enter a denylisted password and verify that the password is rejected or flagged as such.

FIA_PSK_EXT.4 HMAC-Based One-Time Password Pre-shared Keys Support

FIA_PSK_EXT.4.1
TSS
The evaluator shall verify the TSS describes how the HOTP is input into the client and how that value is sent to the server.
Guidance
The evaluator shall verify the operational guidance contains any configuration necessary to enable HOTP.

Tests

- Test FIA_PSK_EXT.4.1:1: The evaluator shall configure the TOE to use a supported HOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the HOTP before initiating the connection. The evaluator shall verify the server validates the HOTP or receives confirmation from an authentication server before establishing the channel.

FIA_PSK_EXT.5 Time-Based One-Time Password Pre-shared Keys Support

FIA_PSK_EXT.5.1
TSS
The evaluator shall verify the TSS describes how the TOTP is input into the client and how that value is sent

to the server.
Guidance
The evaluator shall verify the operational guidance contains any configuration necessary to enable TOTP.

Tests

- Test FIA_PSK_EXT.5.1:1: The evaluator shall configure the TOE to use a supported TOTP factor, then attempt to establish a connection using that factor. The evaluator shall verify the client prompts the user for the TOTP before initiating the connection. The evaluator shall verify the server validates the TOTP or receives confirmation from an authentication server before establishing the channel.

2.8 Evaluation Activities for Objective SFRs

2.8.1 Security Audit (FAU)

FAU_SEL.1/VPN Selective Audit

FAU_SEL.1.1/VPN
TSS
There are no TSS EAs for this SFR.

Guidance
The evaluator shall review the administrative guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain instructions on how to set the pre-selection or how the VPN gateway will configure the client, as well as explain the syntax (if present) for multi-value pre-selection. The administrative guidance shall also identify the audit data that are always recorded, regardless of the selection criteria currently being enforced.

Tests
The evaluator shall perform the following tests:

- Test FAU_SEL.1.1/VPN:1: For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.
- Test FAU_SEL.1.1/VPN:2: [conditional] If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes), then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

2.9 Evaluation Activities for Implementation-dependent SFRs

2.9.1 Security Audit (FAU)

FAU_GEN.1/VPN Audit Data Generation

FAU_GEN.1/VPN
TSS
The evaluator shall examine the TSS to determine that it describes the auditable events and the component that is responsible for each type of auditable event.

Guidance
The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit data. All audit data format types must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP-Module for VPN Clients is described and that the description of the fields contains the information required in FAU_GEN.1.2/VPN, and the additional information specified in the Auditable Events table of the PP-Module for VPN Clients.

In particular, the evaluator shall ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In the Auditable Events table of the PP-Module for VPN Clients, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.

The evaluator shall also make a determination of the administrative actions that are relevant in the context of the PP-Module for VPN Clients. The TOE may contain functionality that is not evaluated in the context of the PP-Module for VPN Clients because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will

not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance 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 PP-Module for VPN Clients, which thus form the set of “all administrative actions”. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.

For each required auditable event, the evaluator shall examine the operational guidance to determine that it is clear to the reader where each event is generated (e.g. the TSF may generate its own audit logs in one location while the platform-provided auditable events are generated elsewhere).

Tests
The evaluator shall test the TOE’s ability to correctly generate audit data by having the TOE generate audit data in accordance with the EAs associated with the functional requirements in the PP-Module for VPN Clients. Additionally, the evaluator shall test that each administrative action applicable in the context of the PP-Module for VPN Clients is auditable. When verifying the test results, the evaluator shall ensure the audit data generated during testing match the format specified in the guidance and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit data is generated as expected.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base-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 the Base-PP as well. The Base-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 chosen 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.
[GPOS PP]	Protection Profile for General Purpose Operating Systems, Version 4.3, September 27, 2022
[MDF PP]	Protection Profile for Mobile Device Fundamentals, Version 3.3, Version 3.3, September 12, 2022
[MDM PP]	Protection Profile for Mobile Device Management, Version 4.0, April 25, 2019
[App PP]	Protection Profile for Application Software, Version 1.4, October 2021