PP-Module for VPN Gateways

Version: 2.0
2026-01-21
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2019-09-17	Initial publication
1.1	2020-06-18	Compatibility with CPP_ND_V2.2E, incorporation of NIAP Technical Decisions
1.2	2022-03-31	Format conversion, incorporation of NIAP Technical Decisions, TC feedback
1.3	2023-08-16	Incorporation of NIAP Technical Decisions, TC feedback
2.0	2026-01-21	Incorporation of NIAP Technical Decisions, Update to CC:2022

Contents

1 Introduction

1.1 Overview

The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of a virtual private network (VPN) gateway in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PP:

- Network Device collaborative Protection Profile Version 4.0

This Base-PP is valid because a VPN gateway is a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. This is functionality that typically will be implemented by a network device.

A Target of Evaluation (TOE) that conforms to a PP-Configuration containing this PP-Module may be a ‘Distributed TOE’ as defined in the NDcPP; however, the VPN gateway functionality described in this PP-Module should be in a single TOE component. This PP-Module does not prohibit the TOE from implementing other security functionality in a distributed manner. For example, a TOE may have a centralized device that performs VPN gateway and other security functionality (such as intrusion prevention) with a number of distributed nodes that help in the enforcement of the secondary functionality.

1.2 Terms

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

1.2.1 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.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to

	the security objectives for the operational environment. There are no security objectives for the TOE.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
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.

1.2.2 Technical Terms

Headend	A VPN use case where the VPN gateway is establishing VPN connectivity with endpoint VPN clients as opposed to other infrastructure devices (e.g., site-to-site).
Packet Filtering	The process by which an edge network device determines if traffic bound to or from its external network is passed to its destination or dropped.
VPN Gateway	A type of network device that resides at the edge of a private network and permits the establishment of VPN connectivity from computers residing in an external network.
Virtual Private Network (VPN)	A mechanism for overlaying a cryptographically secured network over distributed wide-area networks.

1.3 Compliant Targets of Evaluation

This PP-Module specifically addresses network gateway devices that terminate IPsec VPN tunnels. A compliant VPN gateway is a device composed of hardware and software that is connected to two or more distinct networks and has an infrastructure role in the overall enterprise network. In particular, a VPN gateway establishes a secure tunnel that provides an authenticated and encrypted path to one or more other sites and thereby decreases the risk of exposure of information transiting an untrusted network.

The baseline requirements of this PP-Module are those determined necessary for a multi-site VPN gateway device. A compliant TOE may also contain the ability to act as a headend for remote clients. Because this capability is optional, the remote client-based requirements have been included in Appendix A.

1.3.1 TOE Boundary

The physical boundary for a TOE that conforms to this PP-Module is a hardware appliance that also provides generalized network device functionality, such as auditing, identification and authentication, and cryptographic services for network communications. The TOE's logical boundary includes all functionality required by the claimed Base-PP as well as the VPN functionality and related capabilities that are defined in this PP-Module. Any functionality that is provided by the network device that is not relevant to the security requirements defined by this PP-Module or the Base-PP is considered to be outside the scope of the TOE.

1.4 Use Cases

This PP-Module defines two potential use cases for the VPN gateway TOE, defined below. The first use case will always be applicable for a TOE that conforms to this PP-Module. The second use case defines an optional deployment for the TOE that accompanies the first use case.

[USE CASE 1] Network Device

The VPN gateway is part of the functionality that is provided by a general network device appliance, such as a router or switch, or a device that is dedicated solely to providing multi-site VPN gateway functionality.

[USE CASE 2] Remote Client Headend

The VPN gateway provides the ability to act as a headend for remote clients.

1.5 Package Usage

Functional Package for X.509, Version 1.0

Certificate Verification and Validation Required in FIA_XCU_EXT.1.1

The ST author shall select the options to verify and assert identities in FIA_XCU_EXT.1.1.

Limitations on Signature Algorithms in FIA_X509_EXT.1.1

The TOE must utilize appropriate cryptographic algorithms that conform to CNSA standards. Thus, the TOE shall utilize no other algorithms outside of those specified in RFC 8603 for certificate or CRL signatures. Additionally, the TOE shall not use ECDSA with SHA-512 signatures for OCSP responses, and shall utilize no other algorithms for OCSP responses.

Required Extension Processing in FIA_X509_EXT.1.2

The ST author shall select the option to process the basicConstraints and extendedKeyUsage extensions in FIA_X509_EXT.1.2. If the TOE supports identifiers of types other than an identifier located in the CN (i.e., any identifiers specifically labeled as "CN", or the Distinguished Name), the ST author shall select the option to process the subjectAlternateName extension and the relevant options within the subjectAlternateName extension that correspond to the supported identifier types.

CRL or OCSP-based Revocation Required for FIA_X509_EXT.1.3

The TOE must support revocation that only involves CRL or OCSP. Accordingly, the ST author shall select only from options involving CRL or OCSP in FIA_X509_EXT.1.3 (e.g., the selection to treat all certificates older than a given short timeframe is not an acceptable substitute or alternative for supporting CRL or OCSP).

Connections to CRL or OCSP Servers Required for FIA_X509_EXT.1.4

Because the TOE is required to support CRL or OCSP, the TSF shall support an appropriate mechanism for obtaining revocation status information. In the case of CRL, the ST author shall claim that revocation status information is obtained via network connection to a CRL distribution point. In the case of OCSP, the ST author shall claim that revocation status information is obtained via network connection to an OCSP responder, via OCSP stapling, or via OCSP multi-stapling.

Required Function Claims in FIA_X509_EXT.2.1

The ST author shall ensure that the selections and assignments within FIA_X509_EXT.2.1 reflect the usage of X.509 for IPsec or IKE. Other selections and assignments may be made as appropriate for other TOE functionality.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (conformant) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v2.0
- PP-Module for Intrusion Protection Systems, v2.0

Package Claim

- This PP-Module is Functional Package for X.509, version 1.0 conformant.
- This PP-Module does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment (OE), and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

The following threats defined in this PP-Module extend the threats defined by the Base-PP.

T.DATA_INTEGRITY

Devices on a protected network may be exposed to threats presented by devices located outside the protected network that may attempt to modify the data without authorization or determine the contents of secure communication. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained in the communications may be susceptible to a loss of integrity or confidentiality.

T.NETWORK_ACCESS

Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.

From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.

From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled email servers, or, that access to the mail server must be done over an encrypted link.

T.NETWORK_DISCLOSURE

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.

From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information.

From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.

T.NETWORK_MISUSE

Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.

From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services.

From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.

T.REPLAY_ATTACK

If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions:

- Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome
- No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these

3.2 Assumptions

These assumptions are made on the Operational Environment (OE) in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an OE that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

This PP-Module defines assumptions that extend those defined in the supported Base-PP.
All assumptions for the OE of the Base-PP also apply to this PP-Module.
A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

A.CONNECTIONS

It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.3 Organizational Security Policies

This PP defines no Organizational Security Policies beyond those defined in the claimed Base-PP(s).

4 Security Objectives

4.1 Security Objectives for the Operational Environment

This PP-Module defines environmental security objectives that extend those defined in the supported Base-PP. All objectives for the OE of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

OE.CONNECTIONS

The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
A.CONNECTIONS	OE.CONNECTIONS	The OE objective OE.CONNECTIONS is realized through A.CONNECTIONS.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction

In a PP-Configuration that includes the NDcPP, the VPN gateway is expected to rely on some of the security functions implemented by the network device as a whole and evaluated against the Base-PP. In this case, the following sections describe any modifications that the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.2.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDcPP and relevant to the secure operation of the TOE.

5.1.1.1 Cryptographic Support (FCS)

FCS_COP.1/AEAD: Cryptographic Operation - Authenticated Encryption with Associated Data

This SFR has been modified frmo its definition in the NDcPP to mandate selection of AES-GCM mode and 256-bit key sizes. Other selections may still be made if they are needed for other part of the TSF.

The text of FCS_COP.1.1/AEAD is replaced with:

FCS_COP.1.1/AEAD The TSF shall perform [authenticated encryption with associated data] in accordance with a specified cryptographic algorithm [**selection:** *Cryptographic algorithm*] and cryptographic key sizes [**selection:** *Cryptographic key sizes*] that meet the following: [**selection:** *List of standards*].

The following table provides the allowable choices for completion of the selection operations of FCS_COP.1.1/AEAD. In the last column, an X indicates it is mandatory for the ST author to include this row, and an O indicates that the row is optional and need not be included in the table if the TSF does not perform that function. Note that it is not necessary for the ST author to reproduce this final column in the ST.

Allowable choices for FCS_COP.1/AEAD:

Identifier	Cryptographic algorithm	Cryptographic Key Sizes	List of standards	Mandatory or Optional
AES-CCM	AES in CCM mode with unpredictable, non-repeating nonce, minimum size of 64 bits	256 bits	[**selection:** *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [**selection:** *ISO/IEC 19772:2020 (Clause 7), NIST SP 800-38C*] [CCM]	O
AES-GCM	AES in GCM mode with non-repeating IVs using [**selection:** *deterministic*, *RBG-based*], IV construction; the tag must be of length [**selection:** *96*, *104*, *112*, *120*, *128*] bits.	256 bits	[**selection:** *ISO/IEC 18033-3:2010 (Subclause 5.2), FIPS PUB 197*] [AES] [**selection:** *ISO/IEC 19772:2020 (Clause 10), NIST SP 800-38D*] [GCM]	X

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

This SFR has been modified from its definition in the NDcPP to support this PP-Module's IPsec requirements by mandating support for GCM mode.

The text of the FCS_COP.1.1/DataEncryption is replaced with:

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES operating in **GCM mode as defined in FCS_COP.1/AEAD and** [selection:

- *CBC mode as defined in FCS_COP.1/SKC*
- *CTR mode as defined in FCS_COP.1/SKC*
- *XTS mode as defined in FCS_COP.1/SKC*
- *CCM mode as defined in FCS_COP.1/AEAD*
- ***no other modes***

].

Application Note: Other AES modes are selectable if the TSF uses them for another part of the TSF. A selection for 'no other modes' has been refined into the SFR because it is possible that a TOE may conform to the Base-PP by using AES-GCM exclusively for AES data encryption and decryption.

FCS_IPSEC_EXT.1: IPsec Protocol

This SFR has been modified from its definition in the NDcPP to support this module's IPsec requirements by mandating use of AES-GCM-256 and IKEv2 where applicable. Any element that is not mentioned in this section is unchanged from its definition in the Base-PP.

FCS_IPSEC_EXT.1.4: This element has been modified to require the use of CNSA 1.0-compliant parameters.

The text of FCS_IPSEC_EXT.1.4 is replaced with:

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms **AES-GCM-256 (RFC 4106) and** [***no other algorithms***] together with a Secure Hash Algorithm (SHA)-based HMAC [**selection:** *HMAC-SHA-384, no HMAC algorithm*].

Application Note: SHA-based HMAC is not required since AES-GCM satisfies both confidentiality and integrity functions. IPsec may use a truncated version of the SHA-based HMAC functions contained in the selections. Where a truncated output is used, this is described in the TSS.

FCS_IPSEC_EXT.1.5: This element has been modified from its definition in the NDcPP by choosing only the selection for IKEv2, which is selectable in the original definition of the element. It has also been modified to mandate the selection of RFC 4868 conformance due to the required support for SHA-384.

The text of FCS_IPSEC_EXT.1.5 is replaced with:

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- *IKEv2 as defined in RFC 7296 [**selection:** with no support for NAT traversal, with mandatory support for NAT traversal as specified in RFC 7296, Section 2.23], and [RFC 4868 for hash functions]*

]

FCS_IPSEC_EXT.1.6: This SFR is modified from its definition in the Base-PP to remove support for non-CNSA parameters and algorithms. This includes mandating the use of IKEv2.

The text of FCS_IPSEC_EXT.1.6 is replaced with:

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [*IKEv2*] protocol uses the cryptographic algorithms [*AES-GCM-256 (specified in RFC 5282)*].

Application Note: This element is changed from its definition in the Base-PP to mandate support of 256-bit GCM. AES-GCM implementation for IPsec is specified in RFC 5282.

FCS_IPSEC_EXT.1.7: This element has been modified from its definition in the NDcPP by choosing only the selection for IKEv2, which is selectable in the original definition of the element.

The text of FCS_IPSEC_EXT.1.7 is replaced with:

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- *IKEv2 SA lifetimes can be configured by a Security Administrator based on [**selection:***
  - *number of bytes;*
  - *length of time, where the time values cna be configured between [**assignment:** minimum configurable rekey time] and [**assignment:** maximum configurable rekey time]*

  ]

].

FCS_IPSEC_EXT.1.8: This element has been modified from its definition in the NDcPP by choosing only the selection for IKEv2, which is selectable in the original definition of the element.

The text of FCS_IPSEC_EXT.1.8 is replaced with:

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [**selection:***
    - *number of bytes;*
    - *length of time, where the time values cna be configured between [**assignment:** minimum configurable rekey time] and [**assignment:** maximum configurable rekey time]*

  ]

].

FCS_IPSEC_EXT.1.10: This element has been modified from its definition in the NDcPP by choosing only the selection for IKEv2, which is selectable in the original definition of the element.

The text of FCS_IPSEC_EXT.1.10 is replaced with:

FCS_IPSEC_EXT.1.10 The shall generate nonces used in [*IKEv2*] protocol exchanges of length [***selection:***

- *according to the security strength associated with the negotiated Diffie-Hellman group;*
- *at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash*

].

FCS_IPSEC_EXT.1.11: This element has been modified from its definition in the NDcPP by mandating DH group 20, which is selectable in the original definition of the element. The selectable options have also been restricted to conform with CNSA 1.0 parameters.

The text of FCS_IPSEC_EXT.1.11 is replaced with:

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH groups [

- ***20 (384-bit Random ECP) and [selection: 21 (521-bit Random ECP, no other groups] according to RFC 5114***

] **and** [

- [**selection:** *15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), 18 (8192-bit MODP), no other groups] according to RFC 3526*

].

Application Note: This element has been modified from its definition in the NDcPP by mandating DH group 20, which is selectable in the original definition of the element. Any groups other than 20 that are allowed per the element may be selected by the ST author but they are not required for conformance to this PP-Module.

FCS_IPSEC_EXT.1.12: This element has been modified from its definition in the NDcPP by choosing only the selections for IKEv2, which are selectable in the original definition of the element.

The text of FCS_IPSEC_EXT.1.12 is replaced with:

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [**selection:** *IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [**selection:** *IKEv2 CHILD_SA*] connection.

Application Note: Because this PP-Module only permits the use of 256-bit symmetric algorithms, this requirement will be satisfied by default.

FCS_IPSEC_EXT.1.13: This SFR is modified from its definition in the Base-PP by mandating the use of IKEv2 and its authentication methods.

The text of FCS_IPSEC_EXT.1.13 is replaced with:

FCS_IPSEC_EXT.1.13 The TSF shall ensure that **IKEv2** performs peer authentication using [**selection:** *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [**selection:** *Pre-shared Keys* ***that conform to RFC 8784, Pre-shared Keys transmitted via EAP-TTLS, EAP-TLS,*** *no other method*].

Application Note: At least one public-key-based Peer Authentication method is required in order to conform to this PP-Module; one or more of the public key schemes is chosen by the ST author to reflect what is implemented. The ST author also ensures that appropriate FCS requirements reflecting the algorithms used (and key generation capabilities, if provided) are listed to support those methods. Note that the TSS will elaborate on the way in which these algorithms are to be used.

If a selection with “EAP-TLS” or “EAP-TTLS” is chosen, the selection-based requirement FCS_EAP_EXT.1 must be claimed. When an EAP method is used, verification occurs via an external authentication server. Though EAP-TTLS involves PSKs, FIA_PSK_EXT.1 is not claimed because PSK requirements for EAP-TTLS are addressed instead via the Authentication Server PP.

If “pre-shared keys that conform to RFC 8784” is chosen, the selection-based requirement FIA_PSK_EXT.1 must be claimed.

Multifactor support can be achieved via traffic filtering in accordance with FPF_MFA_EXT.1.

It is acceptable for different use cases to leverage different selections. If this is the case, it must be identified.

FCS_IPSEC_EXT.1.14: This SFR is modified from its definition in the Base-PP to require DN to be supported for certificate reference identifiers.

The text of FCS_IPSEC_EXT.1.14 is replaced with:

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: **Distinguished Name (DN),** [**selection:** *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: FQDN, CN: user FQDN,* ***no other reference identifier types, [assignment: other supported reference identifier types]***].

Application Note: This PP-Module requires DN to be supported for certificate reference identifiers at minimum. Other selections may be made by the ST author but they are not required for conformance to this PP-Module.

5.1.1.2 Security Management (FMT)

FMT_MTD.1/CryptoKeys: Management of TSF Data

This SFR, defined in the NDcPP as selection-based, is mandated for inclusion in this PP-Module because the refinements to FMT_SMF.1 mandate its inclusion. Note that it is also refined to refer specifically to keys and certificates used for VPN operation.

The text of FMT_MTD.1.1/CryptoKeys is replaced with:

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to [*manage*] the [*cryptographic keys* ***and certificates used for VPN operation***] to [*Security Administrators*].

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/VPN	No events specified	N/A
FCS_CKM.1/IKE	No events specified	N/A
FMT_SMF.1/VPN	All administrative actions	No additional information.
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	• Source and destination addresses • Source and destination ports • Transport layer protocol
FPT_FLS.1/SelfTest	No events specified	N/A
FPT_TST_EXT.3	No events specified	N/A
FTP_ITC.1/VPN	Initiation of the trusted channel	No additional information.
	Termination of the trusted channel	No additional information.
	Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channel establishment attempt

5.2.2 Security Audit (FAU)

FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)

FAU_GEN.1.1/VPN

The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions
b. All auditable events for the [*not specified*] level of audit;
c. [*Indication that TSF self-test was completed*
d. *Failure of self-test*
e. *auditable events defined in the Auditable Events for Mandatory Requirements table*].

Application Note: The "Start-up and shutdown of the audit functions" event is identical to the event defined in the Base-PP's iteration of FAU_GEN.1. The TOE is not required to have two separate events for this behavior if there is only a single audit stream that which all audit events use. If the TOE does maintain a separate logging facility for VPN gateway-related behavior, then this event must be addressed for it. Note that if the audit functions cannot be started and stopped separately from the TOE itself, then auditing the start-up and shutdown of the TOE is sufficient to address this.

FAU_GEN.1.2/VPN

The TSF shall record within the audit data at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*additional information defined in the Auditable Events for Mandatory Requirements table for each auditable event, where applicable*].

Application Note: The ST author only needs to include the auditable events that correspond to the SFRs claimed in the ST. The TOE is not required to generate auditable events for selection-based or optional SFRs that it does not claim.

5.2.3 Cryptographic Support (FCS)

FCS_CKM.1/IKE Cryptographic Key Generation (for IKE Peer Authentication)

FCS_CKM.1.1/IKE

The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a specified cryptographic key generation algorithm: *[**selection**: FIPS PUB 186-5, “Digital Signature Standard (DSS),” Appendix B.3 for RSA schemes, FIPS PUB 186-5, “Digital Signature Standard (DSS),” Appendix B.4 for ECDSA schemes, and implementing “NIST curves” P-384] and [**selection**:*

- *FFC Schemes using “safe-prime” groups that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [**selection**: RFC 3526, RFC 7919]*
- *no other key generation algorithm*

] and specified cryptographic key sizes [**assignment**: *key size equivalent to, or greater than, a symmetric key strength of 256 bits*] that meet the following: [*no standard*].

Application Note: The keys that are required to be generated by the TOE through this requirement are intended to be used for the authentication of the VPN peers during the IKEv2 key exchange. FCS_CKM.1 in the Base-PP is intended to be used for mechanisms required by the SFRs in the Base-PP. While it is required that the public key be associated with an identity in an X509v3 certificate, this association is not required to be performed by the TOE, and instead is expected to be performed by a CA in the OE.

As indicated in FCS_IPSEC_EXT.1, the TOE is required to implement RSA, ECDSA, or both for peer authentication.

The generated key strength of 2048-bit RSA keys need to be equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, “Recommendation for Key Management” for information about equivalent key strengths.

5.2.4 Security Management (FMT)

FMT_SMF.1/VPN Specification of Management Functions

FMT_SMF.1.1/VPN

The TSF shall be capable of performing the following management functions [

- *Definition of packet filtering rules*
- *Association of packet filtering rules to network interfaces*
- *Ordering of packet filtering rules by priority*

*[**selection**:*

- *Configuration of remote VPN client session timeout*
- *Configuration of attributes used to deny establishment of remote VPN client sessions*
- *Generation of bit-based pre-shared key*
- *No other capabilities*

]].

Application Note: This SFR defines additional management functions for the TOE beyond what is defined in the Base-PP as FMT_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for “network device management” and “VPN gateway management” to be implemented in separate interfaces.

5.2.5 Packet Filtering (FPF)

FPF_RUL_EXT.1 Packet Filtering Rules

FPF_RUL_EXT.1.1

The TSF shall perform packet filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2

The TSF shall allow the definition of packet filtering rules using the following network protocols and protocol fields: [

- *IPv4 (RFC 791)*
    - *source address*
    - *destination address*
    - *protocol*

- *IPv6 (RFC 8200)*
    - *source address*
    - *destination address*
    - *next header (protocol)*
- *TCP (RFC 793)*
    - *source port*
    - *destination port*
- *UDP (RFC 768)*
    - *source port*
    - *destination port*

].

Application Note: This element identifies the protocols and references the protocol definitions that serve to define to what extent the network traffic can be interpreted by the TOE when importing (receiving network traffic or ingress) and exporting (sending–or forming to be sent–network traffic or egress).
While the protocol formatting specified in the RFCs is still used, many RFCs define behaviors which are no longer considered safe to follow. For example, RFC 792 defined the “Redirect” Internet Control Message Protocol (ICMP) type, which is not considered safe to honor when it might come from an adversary; the “source quench” message, which is insecure because its source cannot be validated.
It also identifies the various attributes that are applicable when constructing rules to be enforced by this requirement – the applicable interface is a property of the TOE and the rest of the identified attributes are defined in the associated RFCs. Note that the Protocol is the IPv4 field (in IPv6 this field is called the “next header”) that identifies the applicable protocol, such as TCP, UDP, ICMP, etc. Also, ‘Interface’ identified above is the external port where the applicable network traffic was received or alternately will be sent.

FPF_RUL_EXT.1.3

The TSF shall allow the following operations to be associated with packet filtering rules: permit and drop with the capability to log the operation.

Application Note: This element defines the operations that can be associated with rules used to match network traffic.

FPF_RUL_EXT.1.4

The TSF shall allow the packet filtering rules to be assigned to each distinct network interface.

Application Note: This element identifies where rules can be assigned. Specifically, a conforming TOE must be able to assign filtering rules specific to each of its available and identifiable distinct network interfaces that handle layer 3 and 4 network traffic. Identifiable means the interface is unique and identifiable within the TOE, and does not necessarily require the interface to be visible from the network perspective (e.g., does not need to have an IP address assigned to it). A distinct network interface is one or more physical connections that share a common logical path into the TOE. For example, the TOE might have a small form-factor pluggable (SFP) port supporting SFP modules that expose a number of physical network ports, but since a common driver is used for all external ports they can be treated as a single distinct network interface.
Note that there could be a separate ruleset for each interface or alternately a shared ruleset that somehow associates rules with specific interfaces.

FPF_RUL_EXT.1.5

The TSF shall process the applicable packet filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: [*Administrator-defined*].

Application Note: This element requires that an administrator is able to define the order in which configured filtering rules are processed for matches.

FPF_RUL_EXT.1.6

The TSF shall drop traffic if a matching rule is not identified.

Application Note: This element requires that the behavior is always to deny network traffic when no rules apply.

5.2.6 Protection of the TSF (FPT)

FPT_FLS.1/SelfTest Failure with Preservation of Secure State (Self-Test Failures)

FPT_FLS.1.1/SelfTest

The TSF shall ~~preserve a secure state~~ **shut down** when the following types of failures occur: [*failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests*].

Application Note: This SFR defines the expected TSF response to failures of the self-tests defined in the Base-PP.

FPT_TST_EXT.3 Self-Test with Defined Methods

FPT_TST_EXT.3.1

The TSF shall run a suite of the following self-tests [*when loaded for execution*] to demonstrate the correct operation of the TSF: [*integrity verification of stored executable code*].

FPT_TST_EXT.3.2

The TSF shall execute the self-testing through [*a TSF-provided cryptographic service specified in FCS_COP.1/SigGen (from [NDcPP])*].

Application Note: This requirement expands upon the self-test requirements defined in the NDcPP by specifying the method by which one of the self-tests is to be performed. “Stored TSF executable code” refers to the entire software image of the device and not just the code related to the VPN gateway functionality defined by this PP-Module.

5.2.7 Trusted Path/Channels (FTP)

FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)

FTP_ITC.1.1/VPN

The TSF shall **be capable of using IPsec to** provide a communication channel between itself and **authorized IT entities supporting VPN communications** 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**.

FTP_ITC.1.2/VPN

The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3/VPN

The TSF shall initiate communication via the trusted channel for [**selection, choose one of**: *remote VPN gateways or peers*, *no functions*].

Application Note: The FTP_ITC.1 requirement in the Base-PP relates to other trusted channel functions. This iteration is specific to IPsec VPN communications.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 3: SFR Rationale

Threat	Addressed by	Rationale
T.DATA_ INTEGRITY	FCS_COP.1/DataEncryption (refined from Base-PP)	Mitigates the threat by encrypting channel data using a specified algorithm.
	FCS_IPSEC_EXT.1 (refined from Base-PP)	Mitigates the threat by utilizing IPsec to verify message confidentiality and integrity.
	FPF_RUL_EXT.1	Mitigates the threat by filtering traffic from outside the protected network.
	FPT_FLS.1/SelfTest	Mitigates the threat by ceasing operations of the TSF if a test or security failure is detected, preventing a failure in secure functionality.
	FPT_TST_EXT.3	Mitigates the threat by executing self tests in a specified, repeatable manner.
	FTP_ITC.1/VPN	Mitigates the threat by transmitting data over a secure VPN connection protected from unauthorized disclosure.
	FTA_VCM_EXT.1 (optional)	Mitigates the threat by assigning a private, internal IP address to VPN clients within the protection of the TSF.
	FTA_SSL.3/VPN (optional)	Mitigates the threat by terminating inactive VPN sessions.
T.NETWORK_ ACCESS	FCS_IPSEC_EXT.1 (refined from Base-PP)	Mitigates the threat by utilizing IPsec to create VPN connections for authorized users to access the internal network.
	FIA_X509_EXT.1 (refined from Functional Package for X.509, version 1.0)	Mitigates the threat by preventing connection to servers or clients with malformed or invalid X.509 certificates.

	FIA_X509_EXT.2 (refined from Functional Package for X.509, version 1.0)	Mitigates the threat by authenticating a remote entity using X.509 certificates.
	FIA_X509_EXT.3 (refined from Functional Package for X.509, version 1.0)	Mitigates the threat by utilizing a secure certificate request method to obtain a signed certificate.
	FCS_CKM.1/IKE	Mitigates the threat by generating secure keys utilized for IKE peer authentication.
	FPF_RUL_EXT.1	Mitigates the threat by filtering traffic to disallow unauthorized access.
	FPF_MFA_EXT.1 (optional)	Mitigates the threat by providing for multi-factor authentication of VPN clients.
	FTA_SSL.3/VPN (optional)	Mitigates the threat by terminating inactive VPN sessions to prevent potential unauthorized use.
	FTA_TSE.1 (optional)	Mitigates the threat by preventing connection of VPN clients that meet undesirable criteria.
	FTA_VCM_EXT.1 (optional)	Mitigates the threat by assigning a private, internal IP address to VPN clients within the protection of the TSF.
	FCS_EAP_EXT.1 (selection-based)	Mitigates the threat by securely authenticating VPN clients with a remote authentication server.
	FIA_HOTP_EXT.1 (selection-based)	Mitigates the threat by providing a second factor of authentication via hash-based one-time passwords.
	FIA_PSK_EXT.1 (selection-based)	Mitigates the threat by providing a second factor of authentication via a pre-shared key.
	FIA_PSK_EXT.2 (selection-based)	Mitigates the threat by securely and randomly generating a pre-shared key.
	FIA_PSK_EXT.3 (selection-based)	Mitigates the threat by securely deriving a pre-shared key from a password.
	FIA_TOTP_EXT.1 (selection-based)	Mitigates the threat by providing a second factor of authentication via time-based one-time passwords.
T.NETWORK_DISCLOSURE	FPF_RUL_EXT.1	Mitigates the threat by filtering traffic to disallow unauthorized traffic flows.
	FPT_FLS.1/SelfTest	Mitigates the threat by ceasing operations of the TSF if a test or security failure is detected, preventing a failure in traffic filtering.
	FPT_TST_EXT.3	Mitigates the threat by executing self tests in a specified, repeatable manner.

	FTA_VCM_EXT.1 (optional)	Mitigates the threat by assigning a private, internal IP address to VPN clients within the protection of the TSF.
T.NETWORK_ MISUSE	FAU_GEN.1/VPN	Mitigates the threat by logging potential violations of policy.
	FCS_IPSEC_EXT.1	Mitigates the threat by securing traffic originating from or traveling to an authorized user that resides outside the protected network, ensuring that an unauthorized attacker cannot inject their own actions into the protected network.
	FMT_MTD.1/CryptoKeys	Mitigates the threat by implementing a management interface to manage the IPsec parameters so that unprivileged users do not have the ability to misuse its functions.
	FMT_SMF.1/VPN	Mitigates the threat by implementing a management interface that allows for authorized usage of the TOE so that unprivileged users do not have the ability to misuse its functions.
	FPF_RUL_EXT.1	Mitigates the threat by filtering traffic to or from disallowed services.
	FPT_FLS.1/SelfTest	Mitigates the threat by ceasing operations of the TSF if a test or security failure is detected, preventing a failure in detection or prevention of network misuse.
	FPT_TST_EXT.3	Mitigates the threat by executing self tests in a specified, repeatable manner.
	FTA_VCM_EXT.1 (optional)	Mitigates the threat by assigning a private, internal IP address to VPN clients within the protection of the TSF.
T.REPLAY_ ATTACK	FCS_COP.1/DataEncryption (refined from Base-PP)	Mitigates the threat by utilizing encryption algorithms to protect data from being sent in cleartext.
	FCS_IPSEC_EXT.1 (refined from Base-PP)	Mitigates the threat by utilizing the IPsec protocol to encapsulate and encrypt channel data.
	FPT_FLS.1/SelfTest	Mitigates the threat by ceasing operations of the TSF if a test or security failure is detected, preventing a failure in detection of replay attacks.
	FPT_TST_EXT.3	Mitigates the threat by executing self tests in a specified, repeatable manner.

FTP_ITC.1/VPN	Mitigates the threat by ensuring the channel data (in this case, VPN data) is protected from unauthorized disclosure.
FTA_TSE.1 (optional)	Mitigates the threat by preventing connection from a VPN client that meets undesirable criteria.

6 Consistency Rationale

6.1 Collaborative Protection Profile for Network Devices

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include VPN gateway functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats, assumptions, and organizational security policies (OSPs) defined by this PP-Module (see sections 3.1 through 3.3) supplement those defined in the NDcPP as follows:

Table 4: Consistency of Security Problem Definition (NDcPP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.DATA_INTEGRITY	The threat of data integrity compromise is a specific example of the T.WEAK_CRYPTOGRAPHY threat defined in the Base-PP.
T.NETWORK_ACCESS	The threat of a malicious entity accessing protected network resources without authorization is a specific example of the T.UNTRUSTED_COMMUNICATION_CHANNELS threat defined in the Base-PP.
T.NETWORK_DISCLOSURE	Exposure of network devices due to insufficient protection is a specific example of the T.UNTRUSTED_COMMUNICATION_CHANNELS threat defined in the Base-PP.
T.NETWORK_MISUSE	Depending on the specific nature of the misuse of network resources, this threat is a specific manifestation of either the T.UNTRUSTED_COMMUNICATION_CHANNELS or T.WEAK_AUTHENTICATION_ENDPOINTS threat defined in the Base-PP.
T.REPLAY_ATTACK	A replay attack is mentioned in the Base-PP as a specific type of attack based on the T.UNTRUSTED_COMMUNICATION_CHANNELS threat.
A.CONNECTIONS	This assumption defines the TOE's placement in a network such that it is able to perform its required security functionality. The Base-PP does not define any assumptions about the TOE's architectural deployment so there is no conflict here.

6.1.3 Consistency of OE Objectives

Table 5: Consistency of OE Objectives (NDcPP base)

PP-Module OE Objective	Consistency Rationale

OE.CONNECTIONS	This objective intends for the TOE to be connected to environmental networks in such a way that its primary functionality can be appropriately enforced. There is no inconsistency here with respect to the Base-PP because the Base-PP does not define any restrictions on how a network device is connected to its environment.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support VPN Gateway functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDcPP that are used entirely to provide functionality for VPN Gateways. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 6: Consistency of Requirements (NDcPP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FCS_COP.1/AEAD	This PP-Module mandates a specific selection to be made in this SFR, which does not conflict with the Base-PP because the required selection is an option originally defined in it.
FCS_COP.1/DataEncryption	This PP-Module restricts the Base-PP SFR to a subset of existing permissible functionality and does not introduce any new behavior.
FCS_IPSEC_EXT.1	This PP-Module restricts the Base-PP SFR to a subset of existing permissible functionality and does not introduce any new behavior.
FMT_MTD.1/CryptoKeys	This PP-Module applies the key management functionality already defined in the Base-PP specifically to functionality related to VPN gateways.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
FAU_GEN.1/VPN	This SFR adds new auditable events for the TOE that relate to the functionality that is introduced by the PP-Module.
FCS_CKM.1/IKE	This PP-Module specifies a method of key generation that is not defined in the Base-PP. This is used for functionality defined in the Base-PP (IKE) that this PP-Module chooses to represent in greater detail.
FMT_SMF.1/VPN	This SFR defines management functions that are specific to the functionality required by this PP-Module and were therefore not already defined in the Base-PP iteration of it.
FPF_RUL_EXT.1	This SFR defines specific behavior for the processing of network traffic, specifically which communications channel is used based on certain attributes of the traffic. The Base-PP does not apply any constraints on how usage of a trusted channel is controlled so this does not contradict anything presented in the Base-PP.

FPT_FLS.1/SelfTest	The Base-PP already requires the TOE to specify the self-tests that are performed. This PP-Module simply goes one step further and requires the TSF to behave in a certain way upon failure of those self-tests.
FPT_TST_EXT.3	This PP-Module adds to the self-testing requirements from the Base-PP by mandating that a specific self-test be performed and that it be performed in a certain manner. This does not conflict with the Base-PP because the method used to perform the self-test is a cryptographic function already mandated by the Base-PP.
FTP_ITC.1/VPN	This PP-Module iterates a Base-PP SFR to refer to an interface that is unique to the PP-Module. This does not affect the ability of the Base-PP iteration of the SFR to be satisfied.
Optional SFRs	
FPF_MFA_EXT.1	This SFR relates specifically to the handling of traffic that is used for the establishment of IPsec connections.
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
FTA_SSL.3/VPN	This SFR refers to a specific condition under which a trusted channel is terminated by the TSF. The Base-PP supports termination of trusted channels and does not mandate this be done in any particular method.
FTA_TSE.1	This SFR refers to a specific condition under which a trusted channel is terminated by the TSF. The Base-PP supports termination of trusted channels and does not mandate this be done in any particular method.
FTA_VCM_EXT.1	This SFR refers to network addressing, which is outside the scope of the Base-PP and therefore not prohibited by it.
Selection-based SFRs	
FCS_EAP_EXT.1	This SFR defines the use of EAP-TLS/TTLS; the Base-PP already defines requirements for TLS so potential support for EAP-TLS is consistent with functionality that the Base-PP already expects the TOE may have.
FIA_HOTP_EXT.1	This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.
FIA_PSK_EXT.1	This SFR defines the use of pre-shared keys, which is behavior that only relates to the establishment of IPsec connections.
FIA_PSK_EXT.2	This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.
FIA_PSK_EXT.3	This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

FIA_TOTP_EXT.1	This SFR relates to use of pre-shared keys, which is behavior that only applies to the establishment of IPsec connections.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 Auditable Events for Strictly Optional SFRs

Table 7: Auditable Events for Strictly Optional Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FPF_MFA_EXT.1	No events specified	N/A

A.1.2 Packet Filtering (FPF)

The TOE may support multifactor authentication by blocking all other traffic after connection is established until secondary authentication is validated.

FPF_MFA_EXT.1 Multifactor Authentication Filtering

FPF_MFA_EXT.1.1

The TSF shall not forward packets to the internal network until the IKE tunnel has been established, except those necessary to verify additional authentication factors of the client.

FPF_MFA_EXT.1.2

The TSF shall [**selection**: *verify*, *verify via an external authentication server*] additional authentication factors of the client.

Application Note: If "verify" is selected, FIA_PSK_EXT.1 must be claimed.

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

A.3.1 Auditable Events for Implementation-Based SFRs

Table 8: Auditable Events for Implementation-dependent Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL.3/VPN	No events specified	N/A
FTA_TSE.1	No events specified	N/A

FTA_VCM_EXT.1	No events specified	N/A

A.3.2 TOE Access (FTA)

This section contains requirements that may be optionally selected by the ST author for a "headend" VPN gateway device. The requirements in the main body of this PP-Module are those determined necessary for a multi-site VPN gateway appliance. Another application of a VPN appliance is in an architecture that is intended to serve mobile users, by providing a secure means in which a remote client may access a trusted network. These devices provide the capability to manage remote VPN clients (e.g., assigning IP addresses, managing client sessions) that are not necessarily found in VPN gateways that are limited to providing a secure communication path between trusted networks. Rather than mandate that all VPN gateways provide this mobility aspect, the requirements below are specified as an option. What this means is that multi-site VPN gateways do not have to provide these capabilities, but those devices wishing to serve the mobility community should implement the optional requirements from this Appendix in addition to all mandatory and selection-based requirements that apply to them.

FTA_SSL.3/VPN TSF-Initiated Termination (VPN Headend)

FTA_SSL.3.1/VPN

The TSF shall terminate **a remote VPN client** session after [*an Administrator-configurable time interval of session inactivity*].

Application Note: This requirement exists in the NDcPP; however, it is intended to address an interactive administrative session. Here, the requirement applies to a VPN client that has established an SA. After some configurable time period without any activity, the connection between the VPN headend and client is terminated.

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1

The TSF shall be able to deny session establishment **of a remote VPN client session** based on [*location, time, day, [**selection**: no other attributes, [**assignment**: other attributes]]*].

Application Note: For this PP-Module, "location" is defined as the client's IP address.

FTA_VCM_EXT.1 VPN Client Management

FTA_VCM_EXT.1.1

The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

Application Note: For this requirement, the private IP address is one that is internal to the trusted network for which the TOE is the headend.

Appendix B - Selection-based Requirements

B.1 Auditable Events for Selection-based SFRs

Table 9: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FCS_EAP_EXT.1	No events specified	N/A
FIA_HOTP_EXT.1	No events specified	N/A
FIA_PSK_EXT.1	No events specified	N/A
FIA_PSK_EXT.2	No events specified	N/A
FIA_PSK_EXT.3	No events specified	N/A
FIA_TOTP_EXT.1	No events specified	N/A

B.2 Cryptographic Support (FCS)

FCS_EAP_EXT.1 EAP-TLS/TTLS

The inclusion of this selection-based component depends upon selection in FCS_IPSEC_EXT.1.

FCS_EAP_EXT.1.1

The TSF shall support [**selection**: *EAP-TLS as specified in RFC 5216 and updated by RFC 8996, EAP-TTLS as specified in RFC 5281 and updated by RFC 8996*] over a protected channel per FTP_ITC.1 **from the Base-PP** with an authentication server.

FCS_EAP_EXT.1.2

The TSF shall implement EAP-TLS or EAP-TTLS with the TSF as the EAP client, an authentication server as the EAP server, and the VPN peer as the supplicant.

FCS_EAP_EXT.1.3

The TSF shall use the MSK from the [**selection**: *EAP-TLS*, *EAP-TTLS*] response as the IKEv2 shared secret in the authentication payload.

Application Note: This SFR covers the EAP requirements for a client connection to an authentication server. In particular, authentication server functionality implemented in the same device, rather than in an external device, is covered under the Authentication Server PP-Module, and is out of scope for this PP-Module. The MSK derived from EAP is distinct from the PSK. The MSK is substituted in for the IKEv2 shared secret in the AUTH computations.

B.3 Identification and Authentication (FIA)

The TOE may support pre-shared keys for use in the IPsec protocol, and may use pre-shared keys in other protocols as well. PSK in the context of this document refers to generated values, memorized values subject to conditioning, one-time passwords, and combinations as described in FIA_PSK_EXT.1.2.

FIA_HOTP_EXT.1 HMAC-Based One-Time Password Pre-Shared Keys

The inclusion of this selection-based component depends upon selection in FIA_PSK_EXT.1.2.

FIA_HOTP_EXT.1.1

The TSF shall support HMAC-Based One-Time Password (HOTP) authentication in accordance with RFC 4226 to authenticate the user before establishing VPN connection.

FIA_HOTP_EXT.1.2

The TSF shall generate an HOTP seed according to FCS_RBG.1 (from [NDcPP]) of [**selection**: *128*, *256*] bits.

FIA_HOTP_EXT.1.3

The TSF shall generate a new HOTP seed value for each client.

FIA_HOTP_EXT.1.4

The TSF shall use [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive an HOTP hash from the HOTP seed and counter.

FIA_HOTP_EXT.1.5

The TSF shall truncate the HOTP hash per FIA_HOTP_EXT.1.4 to create an HOTP of [**selection**:

- *administrator configurable character length of at least 6*
- *preset character length of [**selection, choose one of**: 6, 7, 8, 9, 10]*

].

FIA_HOTP_EXT.1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA_HOTP_EXT.1.7

The TSF shall not verify HOTP attempts outside of the counter look ahead window of [**selection**: *a configurable value, [**assignment**: a value less than or equal to 3]*] for resynchronization.

FIA_HOTP_EXT.1.8

The TSF shall increment the counter after each successful authentication.

Application Note: The selection FIA_HOTP_EXT.1.4 must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash

message authentication.
In FIA_HOTP_EXT.1.5 the ST author may either provide a configurable character length of at least 6 or a preset size between 6 and 10.
In FIA_HOTP_EXT.1.6 the ST author may select throttle requests, account lockout, or both.
The HOTP seed and all derived values are considered secret keys for purposes of protection.

FIA_PSK_EXT.1 Pre-Shared Key Composition

The inclusion of this selection-based component depends upon selection in FPF_MFA_EXT.1.2.

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for IPsec and [**selection**: *IKEv2*, *multifactor authentication filtering*].

Application Note: If "IKEv2" is selected, then the corresponding IKEv2 selection must be made in FCS_IPSEC_EXT.1.13. If "multifactor authentication filtering" is selected, then "verify" should be selected in FPF_MFA_EXT.1.2.

FIA_PSK_EXT.1.2

The TSF shall be able to accept the following as pre-shared keys: [**selection**: *generated bit-based*, *password-based*, *HMAC-based one-time password*, *time-based one-time password*, *combination of a generated bit-based and HMAC-based one-time password*, *combination of a generated bit-based and time-based one-time password*, *combination of a password-based and HMAC-based one-time password*, *Combination of a password-based and time-based one-time password*] keys.

Application Note: This requirement is included if "pre-shared keys that conform to RFC 8784" is selected in FCS_IPSEC_EXT.1.13, or if "verify" is selected in FPF_MFA_EXT.1.2. If these selections are made in both FCS_IPSEC_EXT.1.13 and FPF_MFA_EXT.1.2, the TSF must satisfy the appropriate FIA_PSK_EXT.1 selections for each.

If any selection including "generated bit-based" is chosen, then FIA_PSK_EXT.2 must be included.

If "pre-shared keys that conform to RFC 8784" is selected in FCS_IPSEC_EXT.1.13, a generated, bit-based PSK must be used.

If any selection including Password-based keys is chosen, then FIA_PSK_EXT.3 must be included.

If any selection including HMAC-based one-time password keys is chosen, then FIA_HOTP_EXT.1 must be included.

If any selection including time-based one-time password is chosen, then FIA_TOTP_EXT.1 must be included.

FIA_PSK_EXT.2 Generated Pre-Shared Keys

The inclusion of this selection-based component depends upon selection in FIA_PSK_EXT.1.2.

FIA_PSK_EXT.2.1

The TSF shall be able to [**selection**:

- *accept externally generated pre-shared keys*
- *generate [**selection**: 128, 256] bit-based pre-shared keys via FCS_RBG.1 **(from [NDcPP])**.*

]

Application Note: Generated PSKs are expected to be shared between components via an out of band mechanism.
This requirement is selection dependent on FIA_PSK_EXT.1.

FIA_PSK_EXT.3 Password-Based Pre-Shared Keys

The inclusion of this selection-based component depends upon selection in FIA_PSK_EXT.1.2.

FIA_PSK_EXT.3.1

The TSF shall support a PSK of up to [**assignment**: *positive integer of 64 or more*] characters.

FIA_PSK_EXT.3.2

The TSF shall allow PSKs to be composed of any combination of upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [**selection**: *[**assignment**: other supported special characters], no other characters*]

FIA_PSK_EXT.3.3

The TSF shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC-[*SHA-384, with [**assignment**: positive integer of 4096 or more]*] iterations, and output cryptographic key sizes [*256*] that meet the following: [*NIST SP 800-132*].

FIA_PSK_EXT.3.4

The TSF shall not accept PSKs less than [**selection**: *a value settable by the administrator, [**assignment**: minimum PSK length accepted by the TOE, must be >= 6]*] and greater than the maximum PSK length defined in FIA_PSK_EXT.3.1.

FIA_PSK_EXT.3.5

The TSF shall generate all salts using an RBG that meets FCS_RBG.1 **(from [NDcPP])** and with entropy of [**assignment**: *value equal to or greater than 128*] bits.

FIA_PSK_EXT.3.6

The TSF shall require the PSK to be entered before every initiated connection.

FIA_PSK_EXT.3.7

The TSF shall [**selection**: *provide a password strength meter, check the password against a denylist, perform no action to assist the user in choosing a strong password*].

Application Note: For FIA_PSK_EXT.3.1, the ST author assigns the maximum size of the PSK it supports; it must support at least 64 characters or a length defined by the platform.
For FIA_PSK_EXT.3.2, the ST author assigns any other supported characters; if there are no other supported characters, they should select "no other characters."
For FIA_PSK_EXT.3.3, the ST author selects the parameters based on the PBKDF

used by the TSF.
For FIA_PSK_EXT.3.4 If the minimum length is settable, then the ST author chooses "a value settable by the administrator." If the minimum length is not settable, the ST author fills in the assignment with the minimum length the PSK must be. This requirement is to ensure bounds work properly.
For FIA_PSK_EXT.3.7, the ST author may select one, both, or neither of the functions in alignment with NIST SP 800-63b.
This requirement is selection dependent on FIA_PSK_EXT.1.

FIA_TOTP_EXT.1 Time-Based One-Time Password Pre-Shared Keys

The inclusion of this selection-based component depends upon selection in FIA_PSK_EXT.1.2.

FIA_TOTP_EXT.1.1

The TSF shall support Time-Based One-Time Password (TOTP) authentication in accordance with RFC 6238 to authenticate the user before establishing VPN connection.

FIA_TOTP_EXT.1.2

The TSF shall generate a TOTP seed according to FCS_RBG.1 (from [NDcPP])of [**selection**: *128*, *256*] bits.

FIA_TOTP_EXT.1.3

The TSF shall generate a new TOTP seed for each client.

FIA_TOTP_EXT.1.4

The TSF shall use [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive a TOTP hash from the TOTP seed and current time provided by NTP.

FIA_TOTP_EXT.1.5

The TSF shall truncate the TOTP hash per FIA_TOTP_EXT.1.4 to create a TOTP of [**selection**:

- *administrator configurable character length of at least 6*
- *preset character length of [**selection, choose one of**: 6, 7, 8, 9, 10]*

].

FIA_TOTP_EXT.1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA_TOTP_EXT.1.7

The TSF shall set a time-step size of [**selection**: *a configurable value, [**assignment**: a value less than or equal to 30]*] seconds.

FIA_TOTP_EXT.1.8

The TSF shall not validate a drift of more than [**selection**: *a configurable value*, *[**assignment**: a value less than or equal to 3]*] time-steps.

FIA_TOTP_EXT.1.9

The TSF shall [**selection**: *allow resynchronization by recording time drift within the limit of FIA_TOTP_EXT.1.8*, *not permit resynchronization*].

Application Note: The selection FIA_TOTP_EXT.1.4 must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash message authentication.
In FIA_TOTP_EXT.1.5 the ST author may either provide a configurable character length of at least 6 or a preset size between 6 and 10.
In FIA_TOTP_EXT.1.6 the ST author may select throttle requests, account lockout, or both.
The TOTP seed and all derived values are considered secret keys for purposes of protection.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 10: Extended Component Definitions

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_EAP_EXT EAP-TLS/TTLS
Identification and Authentication (FIA)	FIA_HOTP_EXT HMAC-Based One-Time Password Pre-Shared Keys FIA_PSK_EXT Pre-Shared Key Composition FIA_TOTP_EXT Time-Based One-Time Password Pre-Shared Keys
Packet Filtering (FPF)	FPF_MFA_EXT Multifactor Authentication Filtering FPF_RUL_EXT Packet Filtering Rules
Protection of the TSF (FPT)	FPT_TST_EXT TSF Self-Test
TOE Access (FTA)	FTA_VCM_EXT VPN Client Management

C.2 Extended Component Definitions

C.2.1 Cryptographic Support (FCS)

This PP-Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.1.1 FCS_EAP_EXT EAP-TLS/TTLS

Family Behavior

Components in this family describe the requirements for EAP-TLS/TTLS.

Component Leveling

FCS_EAP_EXT
1

FCS_EAP_EXT.1, EAP-TLS/TTLS, defines the use of EAP-TLS/TTLS.

Management: FCS_EAP_EXT.1

No specific management functions are identified.

Audit: FCS_EAP_EXT.1

There are no auditable events foreseen.

FCS_EAP_EXT.1 EAP-TLS/TTLS

Hierarchical to: No other components.

Dependencies to: FCS_IPSEC_EXT.1 IPsec Protocol

FCS_EAP_EXT.1.1

The TSF shall support [**selection**: *EAP-TLS as specified in RFC 5216 and updated by RFC 8996*, *EAP-TTLS as specified in RFC 5281 and updated by RFC 8996*] over a protected channel per FTP_ITC.1 with an authentication server.

FCS_EAP_EXT.1.2

The TSF shall implement EAP-TLS or EAP-TTLS with the TSF as the EAP client, an authentication server as the EAP server, and the VPN peer as the supplicant.

FCS_EAP_EXT.1.3

The TSF shall use the MSK from the [**selection**: *EAP-TLS*, *EAP-TTLS*] response as the IKEv2 shared secret in the authentication payload.

C.2.2 Identification and Authentication (FIA)

This PP-Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.2.1 FIA_HOTP_EXT HMAC-Based One-Time Password Pre-Shared Keys

Family Behavior

Components in this family define requirements for the use of HMAC-Based One-Time password authentication, including generation methods and usage restrictions.

Component Leveling

FIA_HOTP_EXT.1, HMAC-Based One-Time Password Pre-Shared Keys, defines the implementation of HOTP.

Management: FIA_HOTP_EXT.1

No specific management functions are identified.

Audit: FIA_HOTP_EXT.1

There are no auditable events foreseen.

FIA_HOTP_EXT.1 HMAC-Based One-Time Password Pre-Shared Keys

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FIA_HOTP_EXT.1.1

The TSF shall support HMAC-Based One-Time Password (HOTP) authentication in accordance with RFC 4226 to authenticate the user before establishing VPN connection.

FIA_HOTP_EXT.1.2

The TSF shall generate an HOTP seed according to FCS_RBG.1 of [**selection**: *128*, *256*] bits.

FIA_HOTP_EXT.1.3

The TSF shall generate a new HOTP seed value for each client.

FIA_HOTP_EXT.1.4

The TSF shall use [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive an HOTP hash from the HOTP seed and counter.

FIA_HOTP_EXT.1.5

The TSF shall truncate the HOTP hash per FIA_HOTP_EXT.1.4 to create an HOTP of [**selection**:

- *administrator configurable character length of at least 6*
- *preset character length of [**selection, choose one of**: 6, 7, 8, 9, 10]*

].

FIA_HOTP_EXT.1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA_HOTP_EXT.1.7

The TSF shall not verify HOTP attempts outside of the counter look ahead window of [**selection**: *a configurable value*, *[**assignment**: a value less than or equal to 3]*] for resynchronization.

FIA_HOTP_EXT.1.8

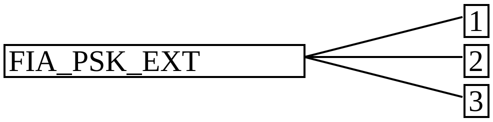
The TSF shall increment the counter after each successful authentication.

C.2.2.2 FIA_PSK_EXT Pre-Shared Key Composition

Family Behavior

This family defines requirements for what the TSF defines or generates as an acceptably strong pre-shared key for authentication.

Component Leveling



FIA_PSK_EXT.1, Pre-Shared Key Composition, defines the use and composition of pre-shared keys used for IPsec.

FIA_PSK_EXT.2, Generated Pre-Shared Keys, defines the use and composition of generated pre-shared keys used for IPsec.

FIA_PSK_EXT.3, Password-Based Pre-Shared Keys, defines the use and composition of password-based pre-shared keys used for IPsec.

Management: FIA_PSK_EXT.1

No specific management functions are identified.

Audit: FIA_PSK_EXT.1

There are no auditable events foreseen.

FIA_PSK_EXT.1 Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies to: FCS_IPSEC_EXT.1 IPsec Protocol

FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for IPsec and [**selection**: *IKEv2*, *multifactor authentication filtering*].

FIA_PSK_EXT.1.2

The TSF shall be able to accept the following as pre-shared keys: [**selection**: *generated bit-based*, *password-based*, *HMAC-based one-time password*, *time-based one-time password*, *combination of a generated bit-based and HMAC-based one-time password*, *combination of a generated bit-based and time-based one-time password*, *combination of a password-based and HMAC-based one-time password*, *combination of a password-based and time-based one-time password*] keys.

Management: FIA_PSK_EXT.2

No specific management functions are identified.

Audit: FIA_PSK_EXT.2

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Failure of the randomization process

FIA_PSK_EXT.2 Generated Pre-Shared Keys

Hierarchical to:	No other components.
Dependencies to:	FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.2.1

The TSF shall be able to [**selection**:

- *accept externally generated pre-shared keys*
- *generate [**selection**: 128, 256] bit-based pre-shared keys via FCS_RBG.1.*

]

Management: FIA_PSK_EXT.3

No specific management functions are identified.

Audit: FIA_PSK_EXT.3

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Failure of the randomization process

FIA_PSK_EXT.3 Password-Based Pre-Shared Keys

Hierarchical to:	No other components.
Dependencies to:	FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.3.1

The TSF shall support a PSK of up to [**assignment**: *positive integer of 64 or more*] characters.

FIA_PSK_EXT.3.2

The TSF shall allow PSKs to be composed of any combination of upper case characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and [**selection**: *[**assignment**: other supported special characters], no other characters*]

FIA_PSK_EXT.3.3

The TSF shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [**assignment**: *cryptographic algorithm*] and output cryptographic key sizes [**assignment**: *output key sizes*] that meet the following: [**assignment**: *applicable standard*].

FIA_PSK_EXT.3.4

The TSF shall not accept PSKs less than [**selection**: *a value settable by the administrator*, *[**assignment**: minimum PSK length accepted by the TOE, must be >= 6]*] and greater than the maximum PSK length defined in FIA_PSK_EXT.3.1.

FIA_PSK_EXT.3.5

The TSF shall generate all salts using an RBG that meets FCS_RBG.1 and with entropy of [**assignment**: *value equal to or greater than 128*] bits.

FIA_PSK_EXT.3.6

The TSF shall require the PSK to be entered before every initiated connection.

FIA_PSK_EXT.3.7

The TSF shall [**selection**: *provide a password strength meter, check the password against a denylist, perform no action to assist the user in choosing a strong password*].

C.2.2.3 FIA_TOTP_EXT Time-Based One-Time Password Pre-Shared Keys

Family Behavior

Components in this family define requirements for the use of Time-Based One-Time password authentication, including generation methods and usage restrictions.

Component Leveling

FIA_TOTP_EXT.1, Time-Based One-Time Password Pre-Shared Keys, defines the implementation of TOTP.

Management: FIA_TOTP_EXT.1

No specific management functions are identified.

Audit: FIA_TOTP_EXT.1

There are no auditable events foreseen.

FIA_TOTP_EXT.1 Time-Based One-Time Password Pre-Shared Keys

Hierarchical to:	No other components.
Dependencies to:	FPT_STM.1 Reliable Time Stamps

FIA_TOTP_EXT.1.1

The TSF shall support Time-Based One-Time Password (TOTP) authentication in accordance with RFC 6238 to authenticate the user before establishing VPN connection.

FIA_TOTP_EXT.1.2

The TSF shall generate a TOTP seed according to FCS_RBG.1 of [**selection**: *128*, *256*] bits.

FIA_TOTP_EXT.1.3

The TSF shall generate a new TOTP seed for each client.

FIA_TOTP_EXT.1.4

The TSF shall use [**selection**: *SHA-1*, *SHA-256*, *SHA-384*, *SHA-512*] with key sizes [**assignment**: *key size (in bits) used in HMAC*] and message digest sizes [**selection**: *160*, *256*, *384*, *512*] to derive a TOTP hash from the TOTP seed and current time provided by NTP.

FIA_TOTP_EXT.1.5

The TSF shall truncate the TOTP hash per FIA_TOTP_EXT.1.4 to create a TOTP of [**selection**:

- *administrator configurable character length of at least 6*
- *preset character length of [**selection, choose one of**: 6, 7, 8, 9, 10]*

].

FIA_TOTP_EXT.1.6

The TSF shall [**selection**:

- *throttle invalid requests to [**selection**: administrator configurable value, [**assignment**: value less than 10]] per minute*
- *lock the associated account after [**selection**: administrator configurable value, [**assignment**: value less than 10]] failed attempts until [**selection**: an administrator unlocks the account, a configurable time period]*

].

FIA_TOTP_EXT.1.7

The TSF shall set a time-step size of [**selection**: *a configurable value, [**assignment**: a value less than or equal to 30]*] seconds.

FIA_TOTP_EXT.1.8

The TSF shall not validate a drift of more than [**selection**: *a configurable value, [**assignment**: a value less than or equal to 3]*] time-steps.

FIA_TOTP_EXT.1.9

The TSF shall [**selection**: *allow resynchronization by recording time drift within the limit of FIA_TOTP_EXT.1.8*, *not permit resynchronization*].

C.2.3 Packet Filtering (FPF)

This class contains families that describe packet filtering behavior. Packet filtering refers to the notion that network traffic that is transmitted through the TOE (i.e., the source and destination of the traffic is not the TOE but the TOE is on the routing path between these two entities) can be treated differently by the TSF based on attributes associated with the traffic. As this class is defined solely to contain an extended component defined for this PP-Module, it has two families, FPF_MFA_EXT and FPF_RUL_EXT.

C.2.3.1 FPF_RUL_EXT Packet Filtering Rules

Family Behavior

This family defines the requirements for the rules that are used to perform packet filtering of network traffic.

Component Leveling

FPF_RUL_EXT.1, Packet Filtering Rules, requires the TSF to enforce a given set of packet filtering rules in an administrator-defined order against one or more TOE interfaces.

Management: FPF_RUL_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure the TOE's packet filtering functionality (i.e., the operations to be performed on network traffic based on configured attributes, the interfaces that these are associated with, and the order in which they are applied).

Audit: FPF_RUL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Application of rules configured with the 'log' operation (including source and destination address, source and destination port, and transport layer protocol value).

FPF_RUL_EXT.1 Packet Filtering Rules

Hierarchical to:	No other components.
Dependencies to:	No dependencies.

FPF_RUL_EXT.1.1

The TSF shall perform packet filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2

The TSF shall allow the definition of packet filtering rules using the following network protocols and protocol fields: [**assignment**: *supported network protocols and protocol fields*].

FPF_RUL_EXT.1.3

The TSF shall allow the following operations to be associated with packet filtering rules: permit and drop with the capability to log the operation.

FPF_RUL_EXT.1.4

The TSF shall allow the packet filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.5

The TSF shall process the applicable packet filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: [**assignment**: *rule processing order*].

FPF_RUL_EXT.1.6

The TSF shall drop traffic if a matching rule is not identified.

C.2.3.2 FPF_MFA_EXT Multifactor Authentication Filtering

Family Behavior

Components in this family describe the requirements for multifactor authentication filtering when using the VPN client.

Component Leveling

FPF_MFA_EXT.1, Multifactor Authentication Filtering, defines the use and composition of multifactor authentication filtering.

Management: FPF_MFA_EXT.1

No specific management functions are identified.

Audit: FPF_MFA_EXT.1

There are no auditable events foreseen.

FPF_MFA_EXT.1 Multifactor Authentication Filtering

Hierarchical to:	No other components.
Dependencies to:	No dependencies.

FPF_MFA_EXT.1.1

The TSF shall not forward packets to the internal network until the IKE tunnel has been established, except those necessary to verify additional authentication factors of the client.

FPF_MFA_EXT.1.2

The TSF shall [**selection**: *verify*, *verify via an external authentication server*] additional authentication factors of the client.

C.2.4 Protection of the TSF (FPT)

This PP-Module defines the following extended components as part of the FPT class originally defined by CC Part 2:

C.2.4.1 FPT_TST_EXT TSF Self-Test

Family Behavior

This family is defined in the Base-PP. This PP-Module augments the extended family by adding one additional component, FPT_TST_EXT.3. This new component and its impact on the extended family's component leveling are shown below; reference the Base-PP for all other definitions for this family.

Component Leveling

FPT_TST_EXT.3, Self-Test with Defined Methods, requires the TSF to specify the methods by which self-testing is performed in addition to identifying the self-tests that are executed and the circumstances in which this execution occurs.

Management: FPT_TST_EXT.3

No specific management functions are identified.

Audit: FPT_TST_EXT.3

There are no auditable events foreseen.

FPT_TST_EXT.3 Self-Test with Defined Methods

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_TST_EXT.3.1

The TSF shall run a suite of the following self-tests [**assignment**: *timing when self-testing is run*] to demonstrate the correct operation of the TSF: [**assignment**: *list of self-tests performed*].

FPT_TST_EXT.3.2

The TSF shall execute the self-testing through [**assignment**: *self-testing mechanism*].

C.2.5 TOE Access (FTA)

This PP-Module defines the following extended components as part of the FTA class originally defined by CC Part 2:

C.2.5.1 FTA_VCM_EXT VPN Client Management

Family Behavior

This family defines requirements for how the TSF interacts with VPN clients in its OE.

Component Leveling

FTA_VCM_EXT
1

FTA_VCM_EXT.1, VPN Client Management, requires the TSF to assign private (internal) IP addresses to VPN clients that successfully establish IPsec connections with it.

Management: FTA_VCM_EXT.1

No specific management functions are identified.

Audit: FTA_VCM_EXT.1

There are no auditable events foreseen.

FTA_VCM_EXT.1 VPN Client Management

Hierarchical to: No other components.

Dependencies to: FCS_IPSEC_EXT.1 IPsec Protocol
[FTP_ITC.1 Inter-TSF Trusted Channel, or

FTP_TRP.1 Trusted Path]

FTA_VCM_EXT.1.1

The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

All SFR dependencies in this PP-Module are addressed by appropriate SFRs, either from elsewhere in the PP-Module or inherited from the Base-PP.

Appendix E - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the Base-PP. As with other Base-PP requirements, the only additional requirement is that the entropy documentation also applies to the specific VPN gateway capabilities of the TOE in addition to the functionality required by the claimed Base-PP.

Appendix F - Acronyms

Table 11: Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CA	Certificate Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CN	Common Name
cPP	Collaborative Protection Profile
DH	Diffie-Hellman
DN	Distinguished Name
FP	Functional Package
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
MSK	Master Session Key
OE	Operational Environment
PBKDF	Password-Based Key Derivation Function
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SA	Security Association
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SFP	Small Form-Factor Pluggable
SFR	Security Functional Requirement

ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
VPN	Virtual Private Network

Appendix G - Bibliography

Table 12: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025