PP-Module for Virtual Private Network (VPN) Gateways

Version: 1.0
2019-09-17
National Information Assurance Partnership

Contents

1. Introduction

1.1 Overview

The scope of this 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-PPs:

- Collaborative Protection Profile for Network Devices (NDcPP) Version 2.1

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 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 provide both Common Criteria and technology terms used in this PP-Module.

1.2.1 Common Criteria Terms

Table 1: CC Terms and Definitions

Term	Definition
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Criteria Testing Laboratory (CCTL)	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.
Protection Profile (PP)	An implementation-independent set of security requirements for a specific category of technology.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Supporting Document (SD)	A companion document to a PP or PP-Module that provides guidance on the specific Evaluation Activities that must be performed in order to evaluate a TOE.

Term	Definition
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 Technology Terms

Table 2: Technology Terms and Definitions

Term	Definition
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 another site(s) 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 within Appendix A.

1.4 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, I&A, 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.

1.5 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/usage model for the TOE that accompanies the first use case.

[USE CASE 1] Network Device

The VPN gateway is part of 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.

2. Conformance Claims

2.1 CC Conformance

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claim

This PP-Module does not claim conformance to any packages.

3. Security Problem Description

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

3.1 Threats

The following threats that are defined in this PP-Module extend the threats that are 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, which may attempt to modify the data without authorization. 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 within the communications may be susceptible to a loss of integrity.

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 e-mail 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 and/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

This PP-Module defines the following assumptions, which extend those defined in the supported Base-PP:

A.CONNECTIONS

It is assumed that 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.

All assumptions for the Operational Environment 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.

3.3 Organizational Security Policies

This PP-Module defines no additional organizational security policies beyond those defined in the Base-PP.

4. Security Objectives

4.1 Security Objectives for the TOE

The following section lists the security objectives for the TOE as well as the functional requirements that are applicable to satisfying these objectives. Note that these mappings include both SFRs from this PP-Module and the Base-PP since the functionality defined in this PP-Module has dependencies on some of the functions defined in the Base-PP.

O.ADDRESS_FILTERING

To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement Packet Filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) and/or receiving (destination) applicable network traffic as well as on established connection information.

Addressed by: FPF_RUL_EXT.1, FTA_VCM_EXT.1 (optional)

O.AUTHENTICATION

To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer and ensure that any such connection attempt is both authenticated and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.

Addressed by: FCS_IPSEC_EXT.1 (refined from Base-PP), FTA_SSL.3/VPN, FTA_TSE.1 (optional), FTP_ITC.1/VPN

O.CRYPTOGRAPHIC_FUNCTIONS

To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement a cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.

Addressed by: FCS_CKM.1/IKE, FCS_COP.1/DataEncryption (refined from Base-PP), FCS_COP.1/SigGen (from Base-PP), FCS_COP.1/Hash (from Base-PP), FCS_COP.1/KeyedHash (from Base-PP), FCS_IPSEC_EXT.1 (refined from Base-PP), FCS_RBG_EXT.1 (from Base-PP), FIA_PSK_EXT.1 (selection-based)

O.FAIL_SECURE

There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.

Addressed by: FPT_FLS.1/SelfTest, FPT_TST_EXT.1 (from Base-PP), FPT_TST_EXT.3, FPT_TUD_EXT.1 (refined from Base-PP)

O.PORT_FILTERING

To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.

Addressed by: FPF_RUL_EXT.1

O.SYSTEM_MONITORING

To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).

Addressed by: FAU_GEN.1 (refined from Base-PP), FPF_RUL_EXT.1

O.TOE_ADMINISTRATION

TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

Addressed by: FIA_AFL.1 (from Base-PP), FIA_UAU_EXT.2 (from Base-PP), FMT_MTD.1/CryptoKeys (refined from Base-PP), FMT_SMF.1 (refined from Base-PP)

4.2 Security Objectives for the Operational Environment

This PP-Module defines the following environmental security objectives, which extend those defined in the supported Base-PP:

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.

All objectives for the Operational Environment 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.

4.3 Security Objectives Rationale

The security objectives defined for the TOE and its operational environment are appropriate to address the security problem based on the following rationale:

Table 3: Security Objective Rationale

Objective	Threat	Rationale
O.ADDRESS_FILTERING	T.DATA_INTEGRITY	The TOE's ability to provide address filtering helps mitigate the threat of data integrity violations by reducing the amount of potentially malicious network traffic that could potentially exploit the threat.
	T.NETWORK_ACCESS	The TOE's address filtering capability helps mitigate the threat of network access by limiting unauthorized reconnaissance activities that can be performed outside the protected network.
	T.NETWORK_DISCLOSURE	The TOE's address filtering capability helps mitigate the threat of network disclosure by limiting unauthorized reconnaissance activities that can be performed outside the protected network.
	T.NETWORK_MISUSE	The TOE's ability to provide address filtering helps mitigate the threat of network misuse by reducing the amount of potentially malicious network traffic that could potentially exploit the threat.
O.AUTHENTICATION	T.DATA_INTEGRITY	The TOE's ability to authenticate entities requesting network access helps mitigate the threat of integrity violations by establishing or exchanging keys that are used to maintain data integrity.
	T.NETWORK_ACCESS	The TOE's ability to authenticate entities requesting network access mitigates unauthorized network access by ensuring that unauthenticated connections cannot access the protected network.
	T.REPLAY_ATTACK	The TOE's ability to enforce authentication helps mitigate replay attacks by making it more difficult for an attacker to impersonate a valid entity.

Objective	Threat	Rationale
O.CRYPTOGRAPHIC_FUNCTIONS	T.DATA_INTEGRITY	The modification of data without authorization can be prevented by cryptography that ensures the confidentiality and integrity of the data.
	T.NETWORK_ACCESS	The TOE's use of cryptography prevents unauthorized network access by encrypting data transmitted to/from an entity on an untrusted network that is accessing a protected resource.
	T.NETWORK_MISUSE	The TOE's use of cryptography prevents network misuse by ensuring that an unauthorized attacker cannot inject their own actions into the protected network.
	T.REPLAY_ATTACK	The TOE's use of cryptography prevents replay attacks by ensuring that network data that is modified and retransmitted will not be parsed as valid traffic.
O.FAIL_SECURE	T.SECURITY_FUNCTIONALITY_FAILURE (from Base-PP)	The TOE's fail-secure mechanism helps further mitigate the security functionality failure threat from the Base-PP by ensuring that the TSF enters a specific and predictable error state if a failure is detected.
O.PORT_FILTERING	T.DATA_INTEGRITY	The TOE's ability to provide port filtering helps mitigate the threat of data integrity violations by reducing the amount of potentially malicious network traffic that could potentially exploit the threat.
	T.NETWORK_ACCESS	The TOE's port filtering capability helps mitigate the threat of network access by limiting unauthorized reconnaissance activities that can be performed outside the protected network.
	T.NETWORK_DISCLOSURE	The TOE's port filtering capability helps mitigate the threat of network disclosure by limiting unauthorized reconnaissance activities that can be performed outside the protected network.

Objective	Threat	Rationale
	T.NETWORK_MISUSE	The TOE's ability to provide port filtering helps mitigate the threat of network misuse by reducing the amount of potentially malicious network traffic that could potentially exploit the threat.
O.SYSTEM_MONITORING	T.NETWORK_MISUSE	The TOE's system monitoring function helps mitigate the threat of network misuse by providing a method to detect when potential misuse is occurring.
	T.UNDETECTED_ACTIVITY (from Base-PP)	The TOE's system monitoring function helps further mitigate the undetected actions threat from the Base-PP by defining additional actions that are detected by the TSF.
O.TOE_ADMINISTRATION	T.UNAUTHORIZED_ADMINISTRATOR _ACCESS (from Base-PP)	The TOE's administration function helps further mitigate the unauthorized actions threat from the Base-PP by defining additional management functions that can only be performed with authorization.

5. Security Requirements

The Security Functional Requirements (SFRs) included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, with additional extended functional components.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignments are indicated with *italicized text*.
- Refinements made by the PP-Module author are indicated with **bold text**. Refinements are only applied to significant technical changes to existing SFRs; minor presentation changes with no technical impact (such as British vs American spelling differences) are not marked as refinements. Refinements are also indicated when an operation is added or substituted for an existing operation (e.g. the PP-Module completes an assignment in such a way that it introduces a selection into the assignment)
- Selections are indicated with *italicized text*.
- Iterations are indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the iteration, e.g. '/VPN' for an SFR relating to VPN functionality.
- Extended SFRs are identified by having a label "EXT" after the SFR name.

Note that selections and assignments to be completed by the ST author are preceded with "selection:" and "assignment:". If text is italicized and does not include either of these, it means that the selection or assignment has already been completed in this PP-Module and the ST author must use the text as written.

5.1 Base-PP 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. The SFRs listed in this section are defined in the Base-PP and relevant to the secure operation of the VPN gateway. This section describes any modifications that the ST author must make to the Base-PP SFRs to satisfy the required VPN gateway functionality.

Note that when an SFR listed in this section omits some elements of a component, it is because this PP-Module prescribes no changes to those elements. They have not been replicated from the Base-PP but still must to be claimed by a conformant TOE.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 is refined to include the following auditable events in addition to what is defined in the Base-PP.

Table 4: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol

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

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in **[*selection: CBC, GCM*] and [*selection: CTR, no other*]** mode and cryptographic key sizes **[*selection: 128 bits, 256 bits*], and [*selection: 192 bits, no other cryptographic key sizes*]** that meet the following: AES as specified in ISO 18033-3, **[*selection: CBC as specified in ISO 10116, GCM as specified in ISO 19772*] and [*selection: CTR as specified in ISO 10116, no other standards*]**.

Application Note: *This SFR has been modified from its definition in the NDcPP to support this PP-Module's IPsec requirements by mandating support for at least one of CBC or GCM modes and at least one of 128-bit or 256-bit key sizes at minimum. Other selections may be made by the ST author but they are not required for conformance to this PP-Module.*

FCS_IPSEC_EXT.1 Internet Protocol Security (IPsec) Communications

This is specified as a selection-based SFR in the Base-PP but is mandatory for any TOE that claims conformance to this PP-Module because IPsec is used to implement the VPN functionality required by the PP-Module.

FCS_IPSEC_EXT.1.3 The TSF shall implement [*selection: transport mode, tunnel mode*].

Application Note: *The selection of supported modes is expected to be performed according to RFC4301.*

This SFR is unchanged from the Base-PP. However, it has been included here to note that future versions of this PP-Module will require that the TSF implement both tunnel mode and transport mode.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms **[*selection: AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 4106)*] and [*selection: AES-CBC-192 (specified in RFC 3602), AES-GCM-192 (specified in RFC 4106), no other algorithm*]** together with a Secure Hash Algorithm (SHA)-based HMAC [*selection:*

HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, no other algorithm].

Application Note: *This SFR element has been modified from its definition in the NDcPP by mandating either 128 or 256 bit key sizes for AES-CBC or AES-GCM, thereby disallowing for the sole selection of 192 bit key sizes.*

When an AES-CBC algorithm is selected, at least one SHA-based HMAC must also be chosen. If only an AES-GCM algorithm is selected, then a SHA-based HMAC is not required since AES-GCM satisfies both confidentiality and integrity functions. IPsec may utilize a truncated version of the SHA-based HMAC functions contained in the selections. Where a truncated output is utilized, this is described in the TSS.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH **Groups 19 (256-bit Random ECP), 20 (384-bit Random ECP, and [*selection: 14 (2048-bit MODP), 24 (2048-bit MODP with 256-bit POS), 15 (3072-bit MODP), no other DH Groups*]**.

Application Note: *This SFR element has been modified from its definition in the NDcPP by mandating DH groups 19 and 20, both of which are selectable in the original definition of the element, and by adding DH group 15 as a new selection. Any groups other than 19 and 20 may be selected by the ST author but they are not required for conformance to this PP-Module.*

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: Fully Qualified Domain Name (FQDN), CN: user FQDN, no other reference identifier type, [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.*

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **IPsec and [*selection: DTLS, HTTPS, SSH, TLS, no other protocols*]**, and [*selection: code signing for system software updates, code signing for integrity verification, [assignment: other uses], no additional uses*].

Application Note: *The Base-PP allows the ST author to specify the TSF's use of X.509 certificates. Because this PP-Module mandates IPsec functionality, the SFR has been refined to force the inclusion of it. Other functions specified by the Base-PP may be chosen without restriction.*

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*selection: device-specific information, Common Name, Organization, Organizational Unit,*

Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

Application Note: *The Base-PP defines this SFR as selection-based with its inclusion being dependent on the communications protocols that the TSF supports. Since a TOE that conforms to this PP-Module must support IPsec, this SFR is mandatory. Aside from mandating its inclusion in the TOE boundary, this PP-Module does not modify the SFR.*

FMT_MTD.1/CryptoKeys Management of TSF Data

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*].

Application Note: *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.*

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using **digital signature and [selection: hash comparison, no other]** capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- ***Ability to manage the cryptographic keys;***
- ***Ability to configure the cryptographic functionality;***
- ***Ability to configure the lifetime for IPsec SAs;***
- ***Ability to import X.509v3 certificates to the TOE's trust store;***
- ***Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this PP-Module;***
- ***Ability to configure all security management functions identified in other sections of this PP-Module;***

[selection:

- *Ability to start and stop services;*
- *Ability to configure audit behavior;*
- *Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full;*
- *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*

- *Ability to configure thresholds for SSH rekeying;*
- *Ability to configure the interaction between TOE components;*
- *Ability to enable or disable automatic checking for updates or automatic updates;*
- *Ability to re-enable an Administrator account;*
- *Ability to set the time which is used for time-stamps;*
- *Ability to configure NTP;*
- *Ability to configure the reference identifier for the peer;*
- *Ability to manage the TOE's trust store and designate X.509v3 certificates as trust anchors;*
- *No other capabilities]*.

Application Note: *The TOE is required to provide the ability to configure the packet filtering functionality that is specified by FPF_RUL_EXT.1 as well as the IPsec functionality that is specified by the Base-PP. Other selections may be made by the ST author but they are not required for conformance to this PP-Module.*

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [*selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]*] to demonstrate the correct operation of the TSF: **noise source health tests,** [*assignment: list of self-tests run by the TSF*].

Application Note: *This SFR is modified from its definition in the NDcPP by requiring noise source health tests to be performed regardless of what other testing is claimed. It is expected that the behavior of this testing will be described in the entropy documentation. Other self-tests may be defined at the ST author's discretion; note that the Application Note in the NDcPP regarding what other self-tests are expected is still applicable here.*

FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a **digital signature mechanism and [*selection: published hash, no other mechanisms*]** prior to installing those updates.

Application Note: *The NDcPP provides an option for how firmware/software updates can be verified but this PP-Module requires the digital signature method to be selected at minimum. Note that all other options specified in the NDcPP for this component are permitted so it is possible for the TSF to use code signing certificates to validate updates, in which case FPT_TUD_EXT.2 from the Base-PP is also included in the ST.*

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 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 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes;***
- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves]*]**

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 algorithms*]**

and specified cryptographic key sizes [*equivalent to, or greater than, a symmetric key strength of 112 bits*].

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 IKE (either v1 or v2) 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 Certificate Authority in the Operational Environment.*

As indicated in FCS_IPSEC_EXT.1, the TOE is required to implement RSA or 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.

5.2.2 Packet Filtering (FPF)

FPF_RUL_EXT.1 Rules for Packet Filtering

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 2460)
  - 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, RFC792 defined the "Redirect" 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.*

5.2.3 Protection of the TSF (FPT)

FPT_FLS.1/SelfTest Fail Secure (Self-Test Failures)

FPT_FLS.1.1/SelfTest The TSF shall **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 TSF 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*].

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.*

5.2.4 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: remote *VPN gateways/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 Assurance Requirements

This PP-Module does not define any SARs beyond those defined by the Base-PP. It is important to note that these SARs are applied to the entire TOE and not just to the portion of the TOE defined by the PP or PP-Module in which the SARs are located.

This PP-Module does provide specific guidance on how the SARs are evaluated for conformance to this PP-Module. The Supporting Document that accompanies this PP-Module defines the additional Evaluation Activities that are to be performed.

6. Consistency Rationale

6.1 NDcPP Base

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 defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

Table 5: Threat Consistency Rationale

PP-Module Threat	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_DISCOSURE	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.

6.1.3 Consistency of Objectives

The Base-PP does not define any TOE objectives; the TOE objectives that are defined by this PP-Module are all mapped to SFRs defined in the Base-PP and PP-Module. Because of this, consistency of the PP-Module's TOE objectives with the Base-PP is demonstrated in section 6.1.4 below.

This PP-Module defines one environmental objective, OE.CONNECTIONS. This objective defines the expected deployment of the TOE in a network topology; specifically, the TOE must be located at a point in the network where T.NETWORK_DISCLOSURE cannot be exploited simply through routing to network resources over a path that does not include the TOE. The Base-PP does not define any objectives for where in the network topology a network device must be located so this objective does not contradict with the expected usage of a network device as described in the Base-PP.

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 network device is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the

NDcPP as well as new SFRs that are used entirely to provide VPN gateway functionality. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 6: SFR Consistency Rationale

PP-Module Requirement	Consistency Rationale
Modified SFR	
FAU_GEN.1	The Base-PP already requires the TOE to provide an audit mechanism; this PP-Module simply includes additional audit events that this mechanism must generate.
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.
FMT_SMF.1	The Base-PP already requires the TOE to provide management functionality; this PP-Module simply mandates some of the optional management functionality specified in the Base-PP and adds new management functions for the security behavior that is introduced in this PP-Module.
FPT_TUD_EXT.1	This PP-Module restricts the Base-PP SFR to a subset of existing permissible functionality and does not introduce any new behavior.
Mandatory SFRs	
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.
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	
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.

PP-Module Requirement	Consistency Rationale
FTA_TSE.1	This SFR refers to a specific condition under which a trusted channel is rejected by the TSF. The Base-PP supports rejection 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.

A. Optional Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP-Module.

Additionally, there are three other types of requirements specified in Appendices A, B, and C.

The first type (in this Appendix) are requirements that can be included in the ST, but do not have to be in order for a TOE to claim conformance to this PP-Module. The second type (in Appendix B) are requirements based on selections in the body of the PP-Module: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) are components that are not required in order to conform to this PP-Module, but will be included in the baseline requirements in future versions of this PP-Module, so adoption by VPN Client vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and/or Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

A.1 Optional Requirements for VPN Headend Functionality

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 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.

A.1.1 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 a remote administrative interactive session. Here, the requirement applies to a VPN client that has established a SA. After some configurable time period without any activity, the connection between the VPN headend and client is terminated.*

A.1.2 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny 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.*

A.1.3 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.*

B. Selection-Based Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP-Module. There are additional requirements based on selections in the body of the PP-Module: if certain selections are made, then additional requirements below will need to be included.

B.1 Cryptographic Support (FCS)

The TOE may support pre-shared keys for use in the IPsec protocol, and may use pre-shared keys in other protocols as well. There are two types of pre-shared keys that must be supported by the TOE, as specified in the requirements below. The first type is referred to as “text-based pre-shared keys”, which refer to pre-shared keys that are entered by users as a string of characters from a standard character set, similar to a password. Such pre-shared keys must be conditioned so that the string of characters is transformed into a string of bits, which is then used as the key.

The second type is referred to as “bit-based pre-shared keys” (for lack of a standard term); this refers to keys that are either generated by the TSF on a command from the administrator, or input in "direct form" by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning" as was the case for text-based pre-shared keys. An example would be a string of hex digits that represent the bits that comprise the key.

The requirements below mandate that the TOE must support both text-based and bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done either by the TOE or in the operational environment.

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec and [*selection: no other protocols, [assignment: other protocols that use pre-shared keys]*].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- Are 22 characters and [*selection: [assignment: other supported lengths], no other lengths*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [*selection: SHA-1, SHA-256, SHA-512, [assignment: method of conditioning text string]*].

FIA_PSK_EXT.1.4 The TSF shall be able to [*selection: accept, generate (using the random bit generator specified in FCS_RBG_EXT.1)*] bit-based pre-shared keys.

Application Note: *Pre-shared keys are an optional method of peer authentication used in IKE. This SFR is applicable to the TOE if “Pre-shared Keys” is selected in FCS_IPSEC_EXT.1.13 in the Base-PP.*

The random bit generator functionality is provided by the Base-PP.

C. Objective Requirements

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

There are currently no objective requirements defined for this PP-Module.

D. Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

D.1 Background and Scope

This Appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Table 7: Extended Components Definitions

Functional Class	Functional Components
Identification and Authentication (FIA)	FIA_PSK_EXT Pre-Shared Key Composition
Packet Filtering (FPF)	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

D.2 Extended Component Definitions

Class FIA: Identification and Authentication

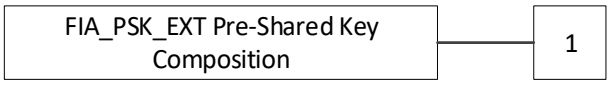
This PP-Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

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, requires the TSF to use only pre-shared keys that meet certain strength requirements.

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: FCS_COP.1 Cryptographic Operation

FCS_IPSEC_EXT.1 Internet Protocol Security (IPsec) Communications

FCS_RBG_EXT.1 Random Bit Generation

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec and [*selection: no other protocols, [assignment: other protocols that use pre-shared keys]*].

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that:

- Are 22 characters and [*selection: [assignment: other supported lengths], no other lengths*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [*selection: SHA-1, SHA-256, SHA-512, [assignment: method of conditioning text string]*].

FIA_PSK_EXT.1.4 The TSF shall be able to [*selection: accept, generate (using the random bit generator specified in FCS_RBG_EXT.1)*] bit-based pre-shared keys.

Class FPF: Packet Filtering

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 only has one family, FPF_RUL_EXT.

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 TSFIs.

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/destination address, source/destination port, and transport layer protocol value)

FPF_RUL_EXT.1 Packet Filtering Rules

Hierarchical to: No other components

Dependencies: 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 protocol fields:

- IPv4 (RFC 791)
  - Source address
  - Destination Address
  - Protocol
- IPv6 (RFC 2460)
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP (RFC 793)
  - Source Port
  - Destination Port
- UDP (RFC 768)
  - Source Port
  - Destination Port

FPF_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with Packet Filtering rules: permit, discard, and log.

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: Administrator-defined.

FPF_RUL_EXT.1.6 The TSF shall drop traffic if a matching rule is not identified.

Class FPT: Protection of the TSF

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

FPT_TST_EXT TSF Self-Test

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, TSF Self-Test with Defined Methods, requires the TSF to specify the method(s) 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

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

- Indication that TSF self-test was completed
- Failure of self-test

FPT_TST_EXT.3 TSF Self-Test with Defined Methods

Hierarchical to: FPT_TST_EXT.1 TSF Self-Test

Dependencies: No dependencies

FPT_TST_EXT.3.1 The TSF shall run a suite of the following self-tests [*selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-tests should occur]*] to demonstrate the correct operation of the TSF: [*assignment: list of self-tests run by the TSF*].

FPT_TST_EXT.3.2 **The TSF shall execute the self-testing through [*assignment: method used to evaluate the success or failure of self-testing*].**

Class FTA: TOE Access

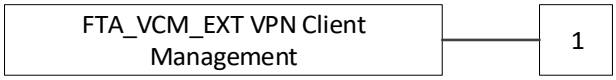
This PP-Module defines the following extended components as part of the FTA class originally defined by CC Part 2:

FTA_VCM_EXT VPN Client Management

Family Behavior

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

Component Leveling



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:	FCS_IPSEC_EXT.1 Internet Protocol Security (IPsec) Communications
	[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.

E. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) 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 that require random data, in addition to any functionality required by the Base-PP.

F. References

Table 8: References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2070-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017 • CC and CEM addenda: Exact Conformance, Selection-Based SFRs, Optional SFRs, CCDB-2017-05-xxx, Version 0.5, May 2017
[NDcPP]	Collaborative Protection Profile for Network Devices, Version 2.1, September 24, 2018
[SD]	Supporting Document Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019

G. Acronyms

The acronym definitions in the NDcPP should be consulted in addition to those defined here.

Table 9: Acronyms

Acronym	Meaning
IKE	Internet Key Exchange
SFP	Small Form-Factor Pluggable
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network