Supporting Document
Mandatory Technical Document

PP-Module for VPN Gateways
Version: 1.2
2022-03-31
National Information Assurance Partnership

Foreword

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

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

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.2	2022-03-31	Format conversion, incorporation of NIAP Technical Decisions, TC feedback
1.1	2020-06-18	Compatibility with CPP_ND_V2.2E, incorporation of NIAP Technical Decisions
1.0	2019-09-17	Initial publication

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

Acknowledgments:
This SD was developed with support from NIAP VPN Gateways Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

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

- Collaborative Protection Profile for Network Devices, Version

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

- VPN Gateways, Version 1.2

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

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

1.2 Structure of the Document

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

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

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

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

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].

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

1.3.2 Technical Terms

	A VPN use case where the VPN gateway is establishing VPN connectivity with endpoint

Headend	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.

2 Evaluation Activities for SFRs

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

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

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

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Collaborative Protection Profile for Network Devices

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

2.1.1 Modified SFRs

2.1.1.1 Cryptographic Support (FCS)

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

FCS_COP.1/DataEncryption
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to require the ST author to make certain selections, but these selections are all part of the original definition of the SFR so no new behavior is defined by the PP-Module.

FCS_IPSEC_EXT.1 IPsec Protocol

FCS_IPSEC_EXT.1
In addition to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document the following activities apply:
TSS
All existing activities regarding "Pre-shared keys" apply to all selections including pre-shared keys. If any selection with "Pre-shared keys" is included, the evaluator shall check to ensure that the TSS describes how the selection works in conjunction with the authentication of IPsec connections.
Guidance
If any selection with "Pre-shared Keys" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.
Tests
There are no additional testing activities.

2.1.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1/Rev
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required support for IPsec.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to support its use for IPsec at a minimum. The evaluator shall ensure that all evaluation of this SFR is performed against its use in IPsec communications as well as any other supported usage.

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required support for IPsec.

2.1.1.3 Security Management (FMT)

FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1/CryptoKeys
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to make it mandatory because of the TOE's required support for IPsec.

2.1.1.4 Protection of the TSF (FPT)

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module requires a particular self-test to be performed, but this self-test is still evaluated using the same methods specified in the Supporting Document.

FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1
There is no change to the Evaluation Activities specified for this SFR in the NDcPP Supporting Document. The PP-Module modifies this SFR to mandate that a particular selection be chosen, but this selection is part of the original definition of the SFR so no new behavior is defined by the PP-Module.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

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

FAU_GEN.1/VPN
TSS
The evaluator shall examine the TSS to verify that it describes the audit mechanisms that the TOE uses to generate audit records for VPN gateway behavior. If any audit mechanisms the TSF uses for this are not used to generate audit records for events defined by FAU_GEN.1 in the Base-PP, the evaluator shall ensure that any VPN gateway-specific audit mechanisms also meet the relevant functional claims from the Base-PP. For example, FAU_STG_EXT.1 requires all audit records to be transmitted to the OE over a trusted channel. This includes the audit records that are required by FAU_GEN.1/VPN. Therefore, if the TOE has an audit mechanism that is only used for VPN gateway functionality, the evaluator shall ensure that the VPN gateway related audit records meet this requirement, even if the mechanism used to generate these audit records does not apply to any of the auditable events defined in the Base-PP.
Guidance
The evaluator shall examine the operational guidance to verify that it identifies all security-relevant auditable events claimed in the ST and includes sample records of each event type. If the TOE uses multiple audit mechanisms to generate different sets of records, the evaluator shall verify that the operational guidance identifies the audit records that are associated with each of the mechanisms such that the source of each audit record type is clear.
Tests
The evaluator shall test the audit functionality by performing actions that trigger each of the claimed audit events and verifying that the audit records are accurate and that their format is consistent with what is specified in the operational guidance. The evaluator may generate these audit events as a consequence of performing other tests that would cause these events to be generated.

2.2.2 Cryptographic Support (FCS)

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

FCS_CKM.1/IKE
TSS
The evaluator shall check to ensure that the TSS describes how the key-pairs are generated. In order to show that the TSF implementation complies with FIPS PUB 186-4, the evaluator shall ensure that the TSS contains the following information:

- The TSS shall list all sections of Appendix B to which the TOE complies
- For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not," "should," and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE
- For each applicable section of Appendix B, any omission of functionality related to "shall" or “should” statements shall be described

Any TOE-specific extensions, processing that is not included in the Appendices, or alternative implementations allowed by the Appendices that may impact the security requirements the TOE is to enforce shall be described.
Guidance
The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.
Tests
For FFC Schemes using “safe-prime” groups:
Testing for FFC Schemes using safe-prime groups is done as part of testing in FCS_CKM.2.
For all other selections:
The evaluator shall perform the corresponding tests for FCS_CKM.1 specified in the NDcPP SD, based on the selections chosen for this SFR. If IKE key generation is implemented by a different algorithm than the NDcPP key generation function, the evaluator shall ensure this testing is performed using the correct implementation.

2.2.3 Security Management (FMT)

FMT_SMF.1/VPN Specification of Management Functions

FMT_SMF.1/VPN
TSS
The evaluator shall examine the TSS to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the TSS identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Guidance
The evaluator shall examine the operational guidance to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the operational guidance identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Tests
The evaluator tests management functions as part of performing other test EAs. No separate testing for FMT_SMF.1/VPN is required unless one of the management functions in FMT_SMF.1.1/VPN has not already been exercised under any other SFR.

2.2.4 Packet Filtering (FPF)

FPF_RUL_EXT.1 Packet Filtering Rules

FPF_RUL_EXT.1.1
TSS
The evaluator shall verify that the TSS provide a description of the TOE’s initialization and startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process.
The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.

Guidance
The operational guidance associated with this requirement is assessed in the subsequent test EAs.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization.
- **Test 2:** The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.

Note: The remaining testing associated with application of the ruleset is addressed in the subsequent test EAs.

FPF_RUL_EXT.1.2
There are no EAs specified for this element. Definition of packet filtering policy, association of operations with packet filtering rules, and association of these rules to network interfaces is described collectively under FPF_RUL_EXT.1.4.
FPF_RUL_EXT.1.3
There are no EAs specified for this element. Definition of packet filtering policy, association of operations with packet filtering rules, and association of these rules to network interfaces is described collectively under FPF_RUL_EXT.1.4.
FPF_RUL_EXT.1.4
TSS
The evaluator shall verify that the TSS describes a packet filtering policy that can use the following fields for each identified protocol, and that the RFCs identified for each protocol are supported:

- 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

The evaluator shall verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing).
The evaluator shall verify that each rule can identify the following actions: permit, discard, and log.
The evaluator shall verify that the TSS identifies all interface types subject to the packet filtering policy and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used), they can be treated collectively as a distinct network interface.

Guidance
The evaluator shall verify that the operational guidance identifies the following protocols as being supported and the following attributes as being configurable within packet filtering rules for the associated protocols:

- IPv4 (RFC 791)
  - 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

The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, discard, and log.
The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces.

The guidance may describe the other protocols contained within the ST (e.g., IPsec, IKE, potentially HTTPS, SSH, and TLS) that are processed by the TOE. The evaluator shall ensure that it is made clear what protocols were not considered as part of the TOE evaluation.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall use the instructions in the operational guidance to test that packet filter rules can be created that permit, discard, and log packets for each of the following attributes:
  - IPv4
    - Destination Address
    - Protocol
  - IPv6
    - Source address
    - Destination Address
    - Next Header (Protocol)
  - TCP
    - Source Port
    - Destination Port
  - UDP
    - Source Port
    - Destination Port
- **Test 2:** The evaluator shall repeat Test 1 above for each distinct network interface type supported by the TOE to ensure that packet filtering rules can be defined for all supported types.

Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the combinations of protocols and attributes required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.

FPF_RUL_EXT.1.5
TSS
The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.

Guidance
The evaluator shall verify that the operational guidance describes how the order of packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall devise two equal packet filtering rules with alternate operations – permit and discard. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.
- **Test 2:** The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g. a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.

FPF_RUL_EXT.1.6
TSS
The evaluator shall verify that the TSS describes the process for applying packet filtering rules and also that the behavior (either by default, or as configured by the administrator) is to discard packets when there is no rule match. The evaluator shall verify the TSS describes when the IPv4 and IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table.

Guidance
The evaluator shall verify that the operational guidance describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the operational guidance provides the appropriate instructions to configure the behavior to discard packets with no matching rules. The evaluator shall verify that the operational guidance describes the range of IPv4 and IPv6 protocols supported by the TOE.

Tests
The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.
- **Test 2:** The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.
- **Test 3:** The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.
- **Test 4:** The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.
- **Test 5:** The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.
- **Test 6:** The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are dropped (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.
- **Test 7:** The evaluator shall configure the TOE to permit and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.
- **Test 8:** The evaluator shall configure the TOE to discard and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.
- **Test 9:** The evaluator shall configure the TOE to permit and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Here the evaluator ensures that the UDP port 500 (IKE) is included in the set of tests.

- **Test 10:** The evaluator shall configure the TOE to discard and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Again, the evaluator ensures that UDP port 500 is included in the set of tests.

The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:

Protocol	Defined Attributes
IPv4	• Transport Layer Protocol 1 - Internet Control Message • Transport Layer Protocol 2 - Internet Group Management • Transport Layer Protocol 3 - Gateway-to-Gateway • Transport Layer Protocol 4 - IP in IP (encapsulation) • Transport Layer Protocol 5 - Stream • Transport Layer Protocol 6 - Transmission Control • Transport Layer Protocol 7 - UCL • Transport Layer Protocol 8 - Exterior Gateway Protocol • Transport Layer Protocol 9 - Any private interior gateway • Transport Layer Protocol 10 - BBN RCC Monitoring • Transport Layer Protocol 11 - Network Voice Protocol • Transport Layer Protocol 12 - PUP • Transport Layer Protocol 13 - ARGUS • Transport Layer Protocol 14 - EMCON • Transport Layer Protocol 15 - Cross Net Debugger • Transport Layer Protocol 16 - Chaos • Transport Layer Protocol 17 - User Datagram • Transport Layer Protocol 18 - Multiplexing • Transport Layer Protocol 19 - DCN Measurement Subsystems • Transport Layer Protocol 20 - Host Monitoring • Transport Layer Protocol 21 - Packet Radio Measurement • Transport Layer Protocol 22 - XEROX NS IDP • Transport Layer Protocol 23 - Trunk-1 • Transport Layer Protocol 24 - Trunk-2 • Transport Layer Protocol 25 - Leaf-1 • Transport Layer Protocol 26 - Leaf-2 • Transport Layer Protocol 27 - Reliable Data Protocol • Transport Layer Protocol 28 - Internet Reliable Transaction • Transport Layer Protocol 29 - ISO Transport Protocol Class 4 • Transport Layer Protocol 30 - Bulk Data Transfer Protocol • Transport Layer Protocol 31 - MFE Network Services Protocol • Transport Layer Protocol 32 - MERIT Internodal Protocol • Transport Layer Protocol 33 - Sequential Exchange Protocol • Transport Layer Protocol 34 - Third Party Connect Protocol • Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol • Transport Layer Protocol 36 - XTP • Transport Layer Protocol 37 - Datagram Delivery Protocol • Transport Layer Protocol 38 - IDPR Control Message Transport Protocol • Transport Layer Protocol 39 - TP++ Transport Protocol • Transport Layer Protocol 40 - IL Transport Protocol • Transport Layer Protocol 41 - Simple Internet Protocol • Transport Layer Protocol 42 - Source Demand Routing Protocol • Transport Layer Protocol 43 - SIP Source Route • Transport Layer Protocol 44 - SIP Fragment • Transport Layer Protocol 45 - Inter-Domain Routing Protocol • Transport Layer Protocol 46 - Reservation Protocol • Transport Layer Protocol 47 - General Routing Encapsulation • Transport Layer Protocol 48 - Mobile Host Routing Protocol • Transport Layer Protocol 49 - BNA • Transport Layer Protocol 50 - SIPP Encap Security Payload • Transport Layer Protocol 51 - SIPP Authentication Header • Transport Layer Protocol 52 - Integrated Net Layer Security TUBA • Transport Layer Protocol 53 - IP with Encryption • Transport Layer Protocol 54 - NBMA Next Hop Resolution Protocol • Transport Layer Protocol 61 - Any host internal protocol • Transport Layer Protocol 62 - CFTP • Transport Layer Protocol 63 - Any local network • Transport Layer Protocol 64 - SATNET and Backroom EXPAK • Transport Layer Protocol 65 - Kryptolan • Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol • Transport Layer Protocol 67 - Internet Pluribus Packet Core • Transport Layer Protocol 68 - Any distributed file system • Transport Layer Protocol 69 - SATNET Monitoring

- Transport Layer Protocol 70 - VISA Protocol
- Transport Layer Protocol 71 - Internet Packet Core Utility
- Transport Layer Protocol 72 - Computer Protocol Network Executive
- Transport Layer Protocol 73 - Computer Protocol Heart Beat
- Transport Layer Protocol 74 - Wang Span Network
- Transport Layer Protocol 75 - Packet Video Protocol
- Transport Layer Protocol 76 - Backroom SATNET Monitoring
- Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary
- Transport Layer Protocol 78 - WIDEBAND Monitoring
- Transport Layer Protocol 79 - WIDEBAND EXPAK
- Transport Layer Protocol 80 - ISO Internet Protocol
- Transport Layer Protocol 81 - VMTP
- Transport Layer Protocol 82 - SECURE-VMTP
- Transport Layer Protocol 83 - VINES
- Transport Layer Protocol 84 - TTP
- Transport Layer Protocol 85 - NSFNET-IGP
- Transport Layer Protocol 86 - Dissimilar Gateway Protocol
- Transport Layer Protocol 87 - TCF
- Transport Layer Protocol 88 - IGRP
- Transport Layer Protocol 89 - OSPFIGP
- Transport Layer Protocol 90 - Sprite RPC Protocol
- Transport Layer Protocol 91 - Locus Address Resolution Protocol
- Transport Layer Protocol 92 - Multicast Transport Protocol
- Transport Layer Protocol 93 - AX.25 Frames
- Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol
- Transport Layer Protocol 95 - Mobile Internetworking Control Protocol
- Transport Layer Protocol 96 - Semaphore Communications Security Protocol
- Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation
- Transport Layer Protocol 98 - Encapsulation Header
- Transport Layer Protocol 99 - Any private encryption scheme
- Transport Layer Protocol 100 - GMTP

- Transport Layer Protocol 1 - Internet Control Message
- Transport Layer Protocol 2 - Internet Group Management
- Transport Layer Protocol 3 - Gateway-to-Gateway
- Transport Layer Protocol 4 - IPv4 encapsulation
- Transport Layer Protocol 5 - Stream
- Transport Layer Protocol 6 - Transmission Control
- Transport Layer Protocol 7 - CBT
- Transport Layer Protocol 8 - Exterior Gateway Protocol
- Transport Layer Protocol 9 - Any private interior gateway
- Transport Layer Protocol 10 - BBN RCC Monitoring
- Transport Layer Protocol 11 - Network Voice Protocol
- Transport Layer Protocol 12 - PUP
- Transport Layer Protocol 13 - ARGUS
- Transport Layer Protocol 14 - EMCON
- Transport Layer Protocol 15 - Cross Net Debugger
- Transport Layer Protocol 16 - Chaos
- Transport Layer Protocol 17 - User Datagram
- Transport Layer Protocol 18 - Multiplexing
- Transport Layer Protocol 19 - DCN Measurement Subsystems
- Transport Layer Protocol 20 - Host Monitoring
- Transport Layer Protocol 21 - Packet Radio Measurement
- Transport Layer Protocol 22 - XEROX NS IDP
- Transport Layer Protocol 23 - Trunk-1
- Transport Layer Protocol 24 - Trunk-2
- Transport Layer Protocol 25 - Leaf-1
- Transport Layer Protocol 26 - Leaf-2
- Transport Layer Protocol 27 - Reliable Data Protocol
- Transport Layer Protocol 28 - Internet Reliable Transaction
- Transport Layer Protocol 29 - Transport Protocol Class 4
- Transport Layer Protocol 30 - Bulk Data Transfer Protocol
- Transport Layer Protocol 31 - MFE Network Services Protocol
- Transport Layer Protocol 32 - MERIT Internodal Protocol
- Transport Layer Protocol 33 - Datagram Congestion Control Protocol
- Transport Layer Protocol 34 - Third Party Connect Protocol
- Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol
- Transport Layer Protocol 36 - XTP
- Transport Layer Protocol 37 - Datagram Delivery Protocol
- Transport Layer Protocol 38 - IDPR Control Message Transport Protocol
- Transport Layer Protocol 39 - TP++ Transport Protocol
- Transport Layer Protocol 40 - IL Transport Protocol
- Transport Layer Protocol 41 - IPv6 encapsulation

IPv6	• Transport Layer Protocol 42 - Source Demand Routing Protocol • Transport Layer Protocol 43 - Intentionally blank • Transport Layer Protocol 44 - Intentionally blank • Transport Layer Protocol 45 - Inter-Domain Routing Protocol • Transport Layer Protocol 46 - Reservation Protocol • Transport Layer Protocol 47 - General Routing Encapsulation • Transport Layer Protocol 48 - Dynamic Source Routing Protocol • Transport Layer Protocol 49 - BNA • Transport Layer Protocol 50 - Intentionally Blank • Transport Layer Protocol 51 - Intentionally Blank • Transport Layer Protocol 52 - Integrated Net Layer Security • Transport Layer Protocol 53 - IP with Encryption • Transport Layer Protocol 54 - NBMA Address Resolution Protocol • Transport Layer Protocol 55 - Mobility • Transport Layer Protocol 56 - Transport Layer Security Protocol using Kryptonet key management • Transport Layer Protocol 57 - SKIP • Transport Layer Protocol 58 - ICMP for IPv6 • Transport Layer Protocol 59 - No Next Header for IPv6 • Transport Layer Protocol 60 - Intentionally Blank • Transport Layer Protocol 61 - Any host internal protocol • Transport Layer Protocol 62 - CFTP • Transport Layer Protocol 63 - Any local network • Transport Layer Protocol 64 - SATNET and Backroom EXPAK • Transport Layer Protocol 65 - Kryptolan • Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol • Transport Layer Protocol 67 - Internet Pluribus Packet Core • Transport Layer Protocol 68 - Any distributed file system • Transport Layer Protocol 69 - SATNET Monitoring • Transport Layer Protocol 70 - VISA Protocol • Transport Layer Protocol 71 - Internet Packet Core Utility • Transport Layer Protocol 72 - Computer Protocol Network Executive • Transport Layer Protocol 73 - Computer Protocol Heart Beat • Transport Layer Protocol 74 - Wang Span Network • Transport Layer Protocol 75 - Packet Video Protocol • Transport Layer Protocol 76 - Backroom SATNET Monitoring • Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary • Transport Layer Protocol 78 - WIDEBAND Monitoring • Transport Layer Protocol 79 - WIDEBAND EXPAK • Transport Layer Protocol 80 - ISO Internet Protocol • Transport Layer Protocol 81 - VMTP • Transport Layer Protocol 82 - SECURE-VMTP • Transport Layer Protocol 83 - VINES • Transport Layer Protocol 84 - TTP • Transport Layer Protocol 85 - Internet Protocol Traffic Manager • Transport Layer Protocol 86 - NSFNET-IGP • Transport Layer Protocol 87 - Dissimilar Gateway Protocol • Transport Layer Protocol 88 - TCF • Transport Layer Protocol 89 - EIGRP • Transport Layer Protocol 90 - OSPFIGP • Transport Layer Protocol 91 - Sprite RPC Protocol • Transport Layer Protocol 92 - Locus Address Resolution Protocol • Transport Layer Protocol 93 - Multicast Transport Protocol • Transport Layer Protocol 94 - AX.25 Frames • Transport Layer Protocol 95 - IP-within-IP Encapsulation Protocol • Transport Layer Protocol 96 - Mobile Internetworking Control Pro. • Transport Layer Protocol 97 - Semaphore Communications Sec. Pro. • Transport Layer Protocol 98 - Ethernet-within-IP Encapsulation • Transport Layer Protocol 99 - Encapsulation Header • Transport Layer Protocol 100 - GMTP • Transport Layer Protocol 101 - Ipsilon Flow Management Protocol • Transport Layer Protocol 102 - PNNI over IP • Transport Layer Protocol 103 - Protocol Independent Multicast • Transport Layer Protocol 104 - ARIS • Transport Layer Protocol 105 - SCPS Transport Layer Protocol • Transport Layer Protocol 106 - QNX • Transport Layer Protocol 107 - Active Networks • Transport Layer Protocol 108 - Payload Compression Protocol • Transport Layer Protocol 109 - Sitara Networks Protocol • Transport Layer Protocol 110 - Compaq Peer Protocol • Transport Layer Protocol 111 - IPX in IP • Transport Layer Protocol 112 - Virtual Router Redundancy Protocol • Transport Layer Protocol 113 - PGM Reliable Transport Protocol • Transport Layer Protocol 114 - Any 0-hop protocol • Transport Layer Protocol 115 - Layer Two Tunneling Protocol

- Transport Layer Protocol 116 - D-II Data Exchange (DDX)
- Transport Layer Protocol 117 - Interactive Agent Transfer Protocol
- Transport Layer Protocol 118 - Schedule Transfer Protocol
- Transport Layer Protocol 119 - SpectraLink Radio Protocol
- Transport Layer Protocol 120 - UTI
- Transport Layer Protocol 121 - Simple Message Protocol
- Transport Layer Protocol 122 - SM
- Transport Layer Protocol 123 - Performance Transparency Protocol
- Transport Layer Protocol 124 - ISIS over IPv4
- Transport Layer Protocol 125 - FIRE
- Transport Layer Protocol 126 - Combat Radio Transport Protocol
- Transport Layer Protocol 127 - Combat Radio User Datagram
- Transport Layer Protocol 128 - SSCOPMCE
- Transport Layer Protocol 129 - IPLT
- Transport Layer Protocol 130 - Secure Packet Shield
- Transport Layer Protocol 131 - Private IP Encapsulation within IP
- Transport Layer Protocol 132 - Stream Control Transmission Protocol
- Transport Layer Protocol 133 - Fibre Channel
- Transport Layer Protocol 134 - RSVP-E2E-IGNORE
- Transport Layer Protocol 135 - Mobility Header
- Transport Layer Protocol 136 - UDPLite
- Transport Layer Protocol 137 - MPLS-in-IP
- Transport Layer Protocol 138 - MANET Protocols
- Transport Layer Protocol 139 - Host Identity Protocol
- Transport Layer Protocol 140 - Shim6 Protocol
- Transport Layer Protocol 141 - Wrapped Encapsulating Security Payload
- Transport Layer Protocol 142 - Robust Header Compression

: RFC Values for IPv4 and IPv6

2.2.5 Protection of the TSF (FPT)

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

FPT_FLS.1/SelfTest
TSS
The evaluator shall ensure the TSS describes how the TOE ensures a shutdown upon a self-test failure, a failed integrity check of the TSF executable image, or a failed health test of the noise source. If there are instances when a shutdown does not occur, (e.g., a failure is deemed non- security relevant), the evaluator shall ensure that those cases are identified and a rationale is provided that supports the classification and justifies why the TOE’s ability to enforce its security policies is not affected in any such instance.
Guidance
The evaluator shall verify that the operational guidance provides information on the self-test failures that can cause the TOE to shut down and how to diagnose the specific failure that has occurred, including possible remediation steps if available.
Tests
There are no test EAs for this component.

FPT_TST_EXT.3 Self-Test with Defined Methods

FPT_TST_EXT.3
TSS
The evaluator shall verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR.
Guidance
There are no guidance EAs for this component.
Tests
There are no test EAs for this component.

2.2.6 Trusted Path/Channels (FTP)

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

FTP_ITC.1/VPN
TSS
The EAs specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.
Guidance
The EAs specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.
Tests

The EAs specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications. Additional testing for IPsec is covered in FCS_IPSEC_EXT.1.

2.3 Evaluation Activities for Optional SFRs

2.3.1 Packet Filtering (FPF)

FPF_MFA_EXT.1 Multifactor Authentication Filtering

FPF_MFA_EXT.1
TSS
The evaluator shall examine the TSS to verify that it describes how authentication packets are identified and how all other traffic is blocked until secondary authentication is successful.
Guidance
The evaluator shall examine the operational guidance to verify that it provides instructions to the administrator on how to configure the secondary HOTP or TOTP factors and any additional details necessary for filtering all other traffic.
Tests

- **Test 1:** For each included selection the evaluator shall configure the TOE per the operational guidance. The evaluator shall attempt to connect and verify other traffic is rejected per the filtering rules. The evaluator shall then provide the selected factor and confirm it is accepted and traffic is no longer blocked.

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Cryptographic Support (FCS)

FCS_EAP_EXT.1 EAP-TLS

FCS_EAP_EXT.1
TSS
The evaluator shall verify that the TSS describes the use of EAP options for each of the selected peer authentication mechanisms, that TLS with mutual authentication is used, that the random values are from an appropriate source, and that the EAP MSK is derived from the TLS master key and is used as the IKEv2 shared key.
Guidance
The evaluator shall verify that the guidance documents describe any configurable features of the EAP or TLS functionality, including instructions for configuration of the authenticators and registration processes for clients.
Tests
Testing for TLS functionality is in accordance with the TLS package. For each supported EAP method claimed in FCS_EAP_EXT.1.1 and for each authentication method claimed in FCS_EAP_EXT.1.3, the evaluator shall perform the following tests:

- **Test 1:** The evaluator shall follow AGD guidance to configure the TSF to use the EAP method claimed. The evaluator shall follow AGD guidance to configure the TSF to use the authentication method claimed and, for EAP-TTLS, register a client with appropriate key material required for the authentication method. The evaluator shall establish a VPN session using a test client with a valid certificate and, for EAP-TTLS, configured to provide a correct value for the configured authenticator. The evaluator shall observe that the VPN session is successful.
- **Test 2:** (conditional for EAP-TTLS support): The evaluator shall cause the test client with a valid certificate to send an invalid authenticator for the claimed authentication method: For HOTP, replay the HOTP value sent previously, For TOTP or PSK, modify a byte of the properly constructed value and observe that the TSF aborts the session.
- **Test 3:** The evaluator shall establish a new, valid certificate for a test client using an identifier not corresponding to a registered user. For EAP-TTLS, the evaluator shall cause the test client using this certificate to send a correct authenticator value for the registered user. The evaluator shall initiate a VPN session from the test client to the TSF and observe that the TSF aborts the session.
- **Test 4:** The evaluator shall follow AGD guidance to configure the TSF to use a supported EAP method and register the user with key material required for a supported authentication method. The evaluator shall configure a test client to respond to an IKE v2 exchange with EAP-request, providing valid phase 1 handshake and valid TLS handshake, but computing the phase 2 shared key using standard (non-EAP) methods. The evaluator shall initiate a VPN session between the test client and the TSF, and observe that the TSF aborts the session.

2.4.2 Identification and Authentication (FIA)

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

FIA_HOTP_EXT.1
TSS

The evaluator shall confirm the TSS describes how the TOE complies with the RFC.
The evaluator shall confirm the TSS describes how the HOTP seed is generated and ensure it aligns with FCS_RBG_EXT.1.
The evaluator shall confirm the TSS describes how the HOTP seed is protected and ensure it aligns with the storage requirements of the Base-PP.
The evaluator shall confirm the TSS describes how a new HOTP seed is assigned for each client and how each client is uniquely identified.
The evaluator shall confirm the TSS describes how the HOTP seed is conditioned into an HOTP hash and verify it matches the selection in FIA_HOTP_EXT.1.4.
The evaluator shall confirm the TSS describes how the HOTP hash is truncated and verify it matches the selection in FIA_HOTP_EXT.1.5.
The evaluator shall confirm the TSS describes how the TOE handles multiple incoming invalid requests and verify it provides an anti-hammer mechanism that matches the selections made in FIA_HOTP_EXT.1.6.
The evaluator shall confirm the TSS describes how the TOE handles resynchronization and how it rejects attempts outside of the look-ahead window selected in FIA_TOTP_EXT.1.7.
The evaluator shall confirm the TSS describes how the TOE counter is incremented after each successful authentication.
Guidance
The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA_HOTP_EXT.1 requirements.
Tests
The evaluator shall configure the TOE to use a supported HOTP factor then:

- **Test 1:** Attempt to establish a connection using a factor from a different client. The test passes if the client fails to connect.
- **Test 2:** Attempt multiple connections outside the limits set in FIA_HOTP_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 3:** Attempt to use an HOTP that is outside of the value allowed for resynchronization. The test passes if the client fails to connect.
- **Test 4:** Attempt to connect with a valid HOTP, disconnect and attempt to authenticate again with the same HOTP value. The test passes if the client connects the first time and fails to connect the second time. If the HOTP generated is duplicated the test may be repeated.

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS
The evaluator shall examine the TSS to ensure that it identifies all protocols that allow pre-shared keys. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states which pre-shared key selections are supported.
Guidance
The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required.
Tests
The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE).

- **Test 1:** For each mechanism selected in FIA_PSK_EXT.1.2 the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection.

FIA_PSK_EXT.2 Generated Pre-Shared Keys

FIA_PSK_EXT.2
TSS
If "generate" is selected, the evaluator shall confirm that this process uses the RBG specified in FCS_RBG_EXT.1 and the output matches the size selected in FIA_PSK_EXT.2.1.
Guidance
The evaluator shall confirm the operational guidance contains instructions for entering generated pre-shared keys for each protocol identified in the FIA_PSK_EXT.1.1.
Tests

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

FIA_PSK_EXT.3 Password-Based Pre-Shared Keys

FIA_PSK_EXT.3
TSS

The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are used.
Support for length: The evaluator shall check to ensure that the TSS describes the allowable ranges for PSK lengths, and that at least 64 characters or a length defined by the platform may be specified by the user.
Support for character set: The evaluator shall check to ensure that the TSS describes the allowable character set and that it contains the characters listed in the SFR.
Support for PBKDF: The evaluator shall examine the TSS to ensure that the use of PBKDF2 is described and that the key sizes match that described by the ST author.
The evaluator shall check that the TSS describes the method by which the PSK is first encoded and then fed to the hash algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself.
For the NIST SP 800-132-based conditioning of the PSK, the required evaluation activities will be performed when doing the evaluation activities for the appropriate requirements (FCS_COP.1/KeyedHash).
The evaluator shall confirm that the minimum length is described.
The ST author shall provide a description in the TSS regarding the salt generation. The evaluator shall confirm that the salt is generated using an RBG described in FCS_RBG_EXT.1.
[conditional] If password strength meter or password denylist is selected, the evaluator shall examine the TSS to ensure any password checking functionality provided by the TSF is described and contains details on how the function operates.

Guidance

The evaluator shall confirm the operational guidance contains instructions for entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall confirm that any management functions related to pre-shared keys that are performed by the TOE are specified in the operational guidance.
The guidance must specify the allowable characters for pre-shared keys, and that list must include, at minimum, the same items contained in FIA_PSK_EXT.3.2.
The evaluator shall confirm the operational guidance contains any necessary instructions for enabling and configuring password checking functionality.

Tests

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

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

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

FIA_PSK_EXT.4

TSS

The evaluator shall verify the TSS describes how the HOTP is input into the client and how that value is sent to the server.
The evaluator shall verify the TSS describes how the HOTP is accepted from an incoming connection and how that value is verified, either by the TOE or by an external authentication server.

Guidance

The evaluator shall verify the operational guidance contains any configuration necessary to enable HOTP.

Tests

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

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

FIA_PSK_EXT.5

TSS

The evaluator shall verify the TSS describes how the TOTP is input into the client and how that value is sent to the server.
The evaluator shall verify the TSS describes how the TOTP is accepted from an incoming connection and how that value is verified, either by the TOE or by an external authentication server.

Guidance

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

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

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

FIA_TOTP_EXT.1
TSS
The evaluator shall confirm the TSS describes how the TOE complies with the RFC.
The evaluator shall confirm the TSS describes how the TOTP seed is generated and ensure it aligns with FCS_RBG_EXT.1.
The evaluator shall confirm the TSS describes how the TOTP seed is protected and ensure it aligns with the storage requirements of the Base-PP.
The evaluator shall confirm the TSS describes how a new TOTP seed is assigned for each client and how each client is uniquely identified.
The evaluator shall confirm the TSS describes how the TOTP seed is conditioned into a TOTP hash and verify it matches the selection in FIA_TOTP_EXT.1.4.
The evaluator shall confirm the TSS describes how the TOTP hash is truncated and verify it matches the selection in FIA_TOTP_EXT.1.5.
The evaluator shall confirm the TSS describes how the TOE handles multiple incoming requests and verify it provides an anti-hammer mechanism that matches the selections made in FIA_TOTP_EXT.1.6.
The evaluator shall confirm the TSS describes how the TOE sets a time-step value and verify it matches the selections in the ST.
The evaluator shall confirm the TSS describes how the TOE handles drift and resynchronization and verify it matches the selections. The evaluator shall ensure the TSS describes how time is kept and whether drift is calculated and recorded. If drift is recorded, the evaluator shall ensure that the TSS describes how this is done.
Guidance
The evaluator shall verify the operational guidance contains all configuration guidance for setting any administrative value that is configurable in the FIA_TOTP_EXT.1 requirements.
Tests
The evaluator shall configure the TOE to use a supported TOTP factor then:

- **Test 1:** Attempt to establish a connection using a factor from a different client. The test passes if the client fails to connect.
- **Test 2:** Attempt multiple connections outside the limits set in FIA_TOTP_EXT.1.6 and verify the remediation is triggered. The test passes if remediation is triggered as defined in the selections and assignments.
- **Test 3:** Attempt to use a TOTP that is outside of the value allowed for resynchronization. The test passes if the client fails to connect.
  Attempt to connect with a valid TOTP, disconnect and attempt to authenticate again with the same TOTP. The test passes if the client connects the first time and fails to connect the second time. If the TOTP generated is duplicated the test may be repeated.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

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

4 Required Supplementary Information

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

Appendix A - References

Identifier	Title

[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2E, March 2020
[ND-SD]	Supporting Document - Mandatory Technical Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019