Supporting Document

Mandatory Technical Document

PP-Module for Virtual Private Network (VPN) Gateways

Version: 1.1

2020-06-18

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:

V1.0 17 September 2019 (Initial)

V1.1 18 June 2020 (updated to extend NDcPP v2.2e)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of Virtual Private Network (VPN) Gateways.

Field of special use:

Virtual Private Network (VPN) Gateways, implemented as network devices.

Acknowledgements:

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

Table of Contents

Tables

1. Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the VPN Gateway 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.

The PP-Module is intended for use with the following Base-PP:

- Protection Profile for Network Devices (NDcPP) Version 2.2e

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

- PP-Module for VPN Gateways, Version 1.1

As such, it defines Evaluation Activities for the functionality described by the VPN Gateway PP-Module as well as any impacts to the Network Device cPP (NDcPP) Evaluation Activities that are required by the PP-Configuration.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they will 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

This document contains modifications and additions to the SD for the NDcPP to accommodate the evaluation of a network device TOE that also provides VPN gateway functionality.

The remainder this section introduces terminology that is relevant to VPN gateway functionality.

Section 2 is divided into two parts. Section 2.1 lists the NDcPP SFRs that are applicable to the VPN gateway functionality and provides instructions for whether the evaluator performs the NDcPP Evaluation Activities for those SFRs as described in the NDcPP SD, or whether any additional or alternative actions are required. Section 2.2 lists the mandatory SFRs added by the VPN Gateway PP-Module and provides Evaluation Activities for them.

Similar to the structure of the NDcPP SD, sections 3-4 identify Evaluation Activities for any optional and selection-based SFRs defined by the PP-Module.

Section 5 identifies Evaluation Activities for any objective SFRs defined by the PP-Module.

Section 6 defines SAR Evaluation Activities for the PP-Module, specifically any cases where the SAR Evaluation Activities must be supplemented to ensure that the VPN gateway portion of the TSF is adequately evaluated.

1.3 Terminology

1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

Supplementary Information

> Information that is not necessarily included in the ST or operational guidance, and that may not necessarily be public. Examples of such information could be entropy analysis, or description of a cryptographic key management architecture used in (or in support of) the TOE. The requirement for any such supplementary information will be identified in the corresponding PP or PP-Module.

Reference the terminology section of [NDcPP] in addition to the acronyms listed below.

Table 1: CC 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.

1.3.2 Acronyms

Reference the acronyms section of [NDcPP] in addition to the acronyms listed below

Table 2: Acronyms

Acronym	Meaning
EA	Evaluation Activity
IKE	Internet Key Exchange
SFP	Small Form-Factor Pluggable
TCP	Transmission Control Property
UDP	User Diagram Protocol
VPN	Virtual Private Network

2. Evaluation Activities for SFRs

The EAs presented in this section are intended to supplement those defined in the NDcPP SD.

The VPN Gateway PP-Module relies on several NDcPP SFRs to help in the implementation of its required functionality. These NDcPP SFRs are listed in this section along with any impact to how they are to be evaluated in a TOE that includes the PP-Module. This section also defines the Evaluation Activities for the mandatory SFRs that are introduced in the PP-Module.

Successful completion of these Evaluation Activities assists in the completion of the relevant portions of ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1, which are required to be applied to the entire TOE.

2.1 NDcPP Evaluation Activities

In addition to the EAs required by the Base-PP, the evaluator shall perform the following additional EAs to ensure that the Base-PP's security functionality is maintained by the addition of the PP-Module. When testing the TOE, it is necessary to ensure these SFRs are tested specifically in conjunction with the VPN gateway portion of the TOE where applicable, either directly or as a dependency to the functionality defined in this PP-Module (e.g., if the TSF has multiple IPsec interfaces and only one of them is used for VPN gateway functionality, testing for FCS_IPSEC_EXT.1 must include tests performed on the VPN gateway interface).

2.1.1 Security Audit (FAU)

2.1.1.1 Security Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit Data Generation

TSS
The evaluator shall verify that the TSS describes how the TSF can be configured to log network traffic associated with applicable rules. Note that this activity may be addressed in conjunction with the TSS Evaluation Activities for FPF_RUL_EXT.1.

The evaluator shall verify that the TSS describes how the TOE behaves when one of its interfaces is overwhelmed by network traffic. It is acceptable for the TOE to drop packets that it cannot process, but under no circumstances is the TOE allowed to pass packets that do not satisfy a rule that allows the permit operation or belong to an allowed established session. It may not always be possible for the TOE to audit dropped packets due to implementation limitations. These limitations and circumstances in which the event of dropped packets is not audited shall be described in the TSS.

The evaluator also verifies that the TSS describes the auditable events for IPsec peer session establishment that are required by the PP-Module.

Operational Guidance
The evaluator shall verify that the operational guidance describes how to configure the TSF to result in applicable network traffic logging. Note that this activity may be addressed in conjunction with the guidance Evaluation Activities for FPF_RUL_EXT.1.

Test
The following test is expected to execute outside the context of the other requirements. While testing the TOE's compliance against the SFRs, either specific tests are developed and run in the context of this SFR,

or as is typically done, the audit capability is turned on while testing the TOE's behavior in complying with the other SFRs in the Base-PP and the PP-Module.

Test 1: The evaluator shall attempt to flood the TOE with network packets such that the TOE will be unable to process all the packets. This may require the evaluator to configure the TOE to limit the bandwidth the TOE is capable to handling (e.g., use of a 10 MB interface). The evaluator shall then review the audit logs to verify that the TOE correctly records that it is unable to process all of the received packets and verify that the TOE logging behavior is consistent with the TSS.

Test 2: The evaluator shall use a remote VPN client to establish an IPsec session with the TOE and observe that the event is logged in accordance with the expectations of the PP-Module.

2.1.2 Cryptographic Support (FCS)

2.1.2.1 Cryptographic Operation (FCS_COP)

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

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.

2.1.2.2 IPsec Protocol (FCS_IPSEC_EXT)

FCS_IPSEC_EXT.1 IPsec Protocol

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.

2.1.3 Identification and Authentication (FIA)

2.1.3.1 Authentication Using X.509 Certificates (FIA_X509_EXT)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

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

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.

2.1.4 Security Management (FMT)

2.1.4.1 Management of TSF Data (FMT_MTD)

FMT_MTD.1/CryptoKeys Management of TSF Data

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 and to state that it applies specifically to the keys and certificates used for VPN operation. The evaluator shall perform the Evaluation Activities as written for this SFR as applicable to the VPN cryptographic data.

2.1.4.2 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

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.

2.1.5 Protection of the TSF (FPT)

2.1.5.1 TSF Self-Test (FPT_TST_EXT)

FPT_TST_EXT.1 TSF Testing

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.

2.1.5.2 Trusted Update (FPT_TUD_EXT)

FPT_TUD_EXT.1 Trusted Update

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 Cryptographic Support (FCS)

2.2.1.1 Cryptographic Key Management (FCS_CKM)

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

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.

Operational 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.

Test
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.

2.2.2 Security Management (FMT)

2.2.2.1 Specification of Management Functions (FMT_SMF)

FMT_SMF.1/VPN Specification of Management Functions (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.

Operational 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.

Test
The evaluator tests management functions as part of testing the SFRs identified in sections 2.2, 3, and 4. 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.

2.2.3 Packet Filtering (FPF)

2.2.3.1 Rules for Packet Filtering (FPF_RUL_EXT.1)

FPF_RUL_EXT.1.1

TSS
The evaluator shall verify that the TSS provide a description of the TOE's initialization/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.

Operational Guidance
The operational guidance associated with this requirement is assessed in the subsequent test Evaluation Activities.

Test
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 Evaluation Activities.

FPF_RUL_EXT.1.2

There are no Evaluation Activities 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 Evaluation Activities 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.

Operational Guidance
The evaluators 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)
  - 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 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.

Test
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
  - Source address
  - 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 each 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 protocol/attribute combinations 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.

Operational 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.

Test
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.

Operational 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.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table below) 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 they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.

Test 2: The evaluator shall configure the TOE to permit all traffic except to discard and log each defined IPv4 Transport Layer Protocol (see table below) 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 they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.

Test 3: The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table below) 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 defined IPv4 Transport Layer Protocol (See table below) 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 IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.

Test 4: The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table below) 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 they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.

Test 5: The evaluator shall configure the TOE to permit all traffic except to discard and log each defined IPv6 Transport Layer Protocol (see table below) 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 they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.

Test 6: The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table below) 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 defined IPv6 Transport Layer Protocol (see table below) 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 they are dropped (i.e., by capturing no applicable packets passing through the TOE) and logged.

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:

Table 3: RFC Values for IPv4 and IPv6

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

Protocol	Defined Attributes
	• 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

Protocol	Defined Attributes
	• 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
IPv6	• 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

Protocol	Defined Attributes
	• 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 • 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

Protocol	Defined Attributes
	• 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

Protocol	Defined Attributes
	• 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

2.2.4 Protection of the TSF (FPT)

2.2.4.1 Fail Secure (FPT_FLS)

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

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 shut-down 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.

Operational 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.

Test
There are no test Evaluation Activities for this SFR.

2.2.4.2 TSF Self-Test (FPT_TST_EXT)

FPT_TST_EXT.3 Self-Test with Defined Methods

TSS
The evaluator verifies 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.

Operational Guidance
There are no operational guidance Evaluation Activities for this SFR.

Test
There are no test Evaluation Activities for this SFR.

2.2.5 Trusted Path/Channels (FTP)

2.2.5.1 Inter-TSF Trusted Channel (FTP_ITC)

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

TSS
The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.

Operational Guidance
The evaluation activities specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.

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

3. Evaluation Activities for Optional Requirements

3.1 TOE Access (FTA)

3.1.1 Session Locking and Termination (FTA_SSL)

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

TSS
The evaluator shall examine the TSS to verify that it describes the ability of the TSF to terminate an inactive VPN client session.

Operational Guidance
The evaluator shall examine the operational guidance to verify that it provides instructions to the administrator on how to configure the time limit for termination of an active VPN client session.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall follow the steps provided in the operational guidance to set the inactivity timer for five minutes. The evaluator shall then connect a VPN client to the TOE, let it sit idle for four minutes and fifty seconds, and observe that the VPN client is still connected at this time by performing an action that would require VPN access. The evaluator shall then disconnect the client, reconnect it, wait five minutes and ten seconds, attempt the same action, and observe that it does not succeed. The evaluator shall then verify using audit log data that the VPN client session lasted for exactly five minutes.

Test 2: The evaluator shall configure the inactivity timer to ten minutes and repeat Test 1, adjusting the waiting periods and expected audit log data accordingly.

3.1.2 TOE Session Establishment (FTA_TSE)

FTA_TSE.1 TOE Session Establishment

TSS
The evaluator shall examine the TSS to verify that it describes the methods by which the TSF can deny the establishment of an otherwise valid remote VPN client session (e.g., client credential is valid, not expired, not revoked, etc.), including day, time, and IP address at a minimum.

Operational Guidance
The evaluator shall review the operational guidance to determine that it provides instructions for how to enable an access restriction that will deny VPN client session establishment for each attribute described in the TSS.

Test
The evaluator shall perform the following tests:

Test 1: The evaluator shall successfully connect a remote VPN client to the TOE and then disconnect it, noting the IP address from which the client connected. The evaluator shall follow the steps described in the operational guidance to prohibit that IP address from connecting, attempt to reconnect using the same VPN client, and observe that it is not successful.

Test 2: The evaluator shall successfully connect a remote VPN client to the TOE and then disconnect it. The evaluator shall follow the steps described in the operational guidance to prohibit the VPN client from connecting on a certain day (whether this is a day of the week or specific calendar date), attempt to reconnect using the same VPN client, and observe that it is not successful.

Test 3: The evaluator shall successfully connect a remote VPN client to the TOE and then disconnect it. The evaluator shall follow the steps described in the operational guidance to prohibit the VPN client during a range of times that includes the time period during which the test occurs, attempt to reconnect using the same VPN client, and observe that it is not successful.

Test 4: [conditional] If any other attributes are identified in FTA_TSE.1, the evaluator shall conduct a test similar to tests 1 through 3 to demonstrate the enforcement of each of these attributes. The evaluator shall demonstrate a successful remote client VPN connection, configure the TSF to deny that connection based on the attribute, and demonstrate that a subsequent connection attempt is unsuccessful.

3.1.3 VPN Client Management (FTA_VCM_EXT)

FTA_VCM_EXT.1 VPN Client Management

TSS
The evaluator shall check the TSS to verify that it asserts the ability of the TSF to assign a private IP address to a connected VPN client.

Operational Guidance
There are no operational guidance Evaluation Activities for this SFR.

Test
The evaluator shall connect a remote VPN client to the TOE and record its IP address as well as the internal IP address of the TOE. The evaluator shall verify that the two IP addresses belong to the same network. The evaluator shall disconnect the remote VPN client and verify that the IP address of its underlying platform is no longer part of the private network identified in the previous step.

4. Evaluation Activities for Selection-Based Requirements

4.1 Identification and Authentication (FIA)

4.1.1 Pre-Shared Key Composition (FIA_PSK_EXT)

FIA_PSK_EXT.1 Pre-Shared Key Composition

TSS

The evaluator shall examine the TSS to ensure that it identifies all protocols that allow both text-based and bit-based pre-shared keys, and states that text-based pre-shared keys of 22 characters are supported. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states the conditioning that takes place to transform the text-based pre- shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by the protocol, and that this conditioning is consistent with the last selection in the FIA_PSK_EXT.1.3 requirement.

Operational Guidance

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

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

Test

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). Note that one or more of these tests can be performed with a single test case.

Test 1: The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.

Test 2 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.

Test 3 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

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

5. Evaluation Activities for Objective Requirements

There are currently no objective requirements defined by the PP-Module.

6. Evaluation Activities for SARs

To evaluate the SARs specified by NDcPP and this PP-Module, the evaluator shall perform the SAR Evaluation Activities defined in the NDcPP SD against the entire TOE (i.e., both the network device portion and the VPN gateway portion). In particular, the evaluator shall ensure that the vulnerability testing defined in section A.1.4 of the NDcPP SD is applied to the TOE's VPN interface(s) in addition to any other security-relevant network device interfaces that the TOE may have.

7. Required Supplementary Information

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

8. References

Table 4: 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
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
[NDcPP SD]	Supporting Document – Mandatory Technical Document – Evaluation Activities for Network Device cPP, Version 2.2, December 2019
[VPNGW]	PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18 June 2020