Australian Government
Department of Defence

ASD-Approved Extended Package

Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPN GW EP)

Version:	**2.0**
Technology type:	**Network related devices**
Authored by:	**Information Assurance Directorate, United States**
Publication date:	**01 December 2015**
ASD approval date:	**30 May 2016**

The following document is a Protection Profile Extended Package authored by Information Assurance Directorate, United States. This collaborative Protection Profile Extended Package has been approved for use by the Australian Signals Directorate.

This Extended Package (EP) describes the security requirements for VPN Gateway. Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by law or regulation.

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

The baseline requirements of this EP are those determined necessary for a multi-site VPN Gateway device. However, a compliant TOE may contain the ability to act as a headend for remote clients. Because this capability is optional, the remote client based requirements have been included within Appendix D.

Since this EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

For information relating to the application of Protection Profiles, please refer to the Australian Government Information Security Manual (ISM) or www.asd.gov.au Controls in the ISM take precedence over any requirements contained in this PP where there is a conflict.

Network Device collaborative Protection Profile (NDcPP) Extended Package
VPN Gateway

Information Assurance Directorate

01 December 2015

Version 2.0

Table of Contents

Revision History

Version	Date	Description
1.0	December 2011	Initial release
1.1	April 2013	Updated X.509 requirements to specify the certificate path validation algorithm must ensure a basicConstraints field is present and the cA flag set to TRUE as a condition that must be met for a certificate to be considered a CA certificate.
1.2	October 2015	Updated to reflect changes to the base PP made as a result of transition from NDPP to NDcPP

1 Introduction

This Extended Package (EP) describes security requirements for a VPN Gateway (defined to be a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network) and is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well defined and described threats. However, this EP is not complete in itself, but rather extends the *collaborative Protection Profile for Network Devices* (NDcPP). This introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDcPP.

1.1 Conformance Claims

The *collaborative Protection Profile for Network Devices* (NDcPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDcPP baseline with additional SFRs and associated 'Assurance Activities' specific to VPN Gateway network infrastructure devices. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

As an EP of the NDcPP, it is expected that the content of both this EP and the NDcPP be appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined such that there should be no difficulty or ambiguity in so doing. An ST must identify the applicable versions of the NDcPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

1.3 Compliant Targets of Evaluation

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

The baseline requirements of this EP are those determined necessary for a multi-site VPN Gateway device. However, a compliant TOE may contain the ability to act as a headend for remote clients. Because this capability is optional, the remote client based requirements have been included within Appendix D.

Since this EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP in response to the threat environment discussed subsequently herein.

It is intended that the set of requirements in this EP is limited in scope in order to promote quicker, less costly evaluations that provide some value to end users.

2 Security Problem Description

VPN Gateways address a range of security threats related to the confidentiality and integrity of data that traverses an untrusted network such as infiltration into a protected network and exfiltration from a protected network. The term *protected network* is used here to represent an attached network for which IPsec rules are defined to control VPN access. As such, a given VPN could potentially have a variety of attached protected and unprotected networks simultaneously depending on its specific configuration. It should also be clear that all attached networks are presumed to be *protectable* at the discretion of an administrator. The term *ingress traffic* is used below to represent traffic from threat agents that exist outside a protected network and the term *egress traffic* is used below to represent traffic from threat agents that exist inside a protected network. Applicable threats include unauthorized disclosure of information, inappropriate access to services, and network-based reconnaissance. However, relative to the data, it does not matter where the threat agent is located. Example: data exfiltration means that data was removed without proper authorization to remove it. This may be a pull or a push. It can result from intrusion from the outside or by the actions of the insider. A site is responsible for developing its security policy and configuring a rule set that the VPN will enforce to meet their needs.

Note that this EP does not repeat the threats identified in the NDcPP, though they all apply given the conformance and hence dependence of this EP on the NDcPP. Note also that while the NDcPP contains only threats to the ability of the TOE to provide its security functions, this EP addresses only business threats to resources in the operational environment. Together the threats of the NDcPP and those defined in this EP define the comprehensive set of security threats addressed by a VPN TOE.

2.1 Unauthorized Disclosure of Information

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

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

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

(T.NETWORK_DISCLOSURE)

2.2 Inappropriate Access to Services

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

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

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

(T. NETWORK_ACCESS)

2.3 Misuse of Services

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

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

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

(T.NETWORK_MISUSE)

2.4 Compromise of Data Integrity

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.

(T.DATA_INTEGRITY)

2.5 Replay Attack

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

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

(T.REPLAY_ATTACK)

3 Security Objectives

The Security Problem described in Section 2 will be addressed by a combination of cryptographic capabilities, and packet filtering. Compliant TOEs will provide security functionality that addresses threats to the TOE and enforces policies that are imposed by law or regulation. The following subsections provide a description of the security objectives required to meet the threats/policies previously discussed. This refers to the objectives that are addressed by this EP and does not include any capabilities from the NDcPP unless they are mandated for inclusion within the TSF when this EP is claimed.

Note: in each subsection below particular security objectives are identified (highlighted by *O.*) and they are matched with the associated security functional requirements (SFRs) that provide the mechanisms to satisfy the objectives.

3.1 Data Encryption and Decryption

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

(O.CRYPTOGRAPHIC_FUNCTIONS → FCS_CKM.1/IKE, FCS_COP.1, FCS_RBG_EXT.1, FCS_IPSEC_EXT.1)

3.2 Authentication

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

(O.AUTHENTICATION → FTP_ITC.1, FCS_IPSEC_EXT.1)

3.3 Address-Based Filtering

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

(O.ADDRESS_FILTERING → FPF_RUL_EXT.1)

3.4 Insecure Operations

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

(O.FAIL_SECURE → FPT_FLS.1/SelfTest, FPT_TST_EXT.1, FPT_TUD_EXT.1)

3.5 Port Based Filtering

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

(O.PORT_FILTERING → FPF_RUL_EXT.1)

3.6 System Monitoring

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

(O.SYSTEM_MONITORING → FAU_GEN.1, FPF_RUL_EXT.1)

3.7 TOE Administration

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

(O.TOE_ADMINISTRATION → FIA_AFL.1, FMT_MOF.1/AdminAct, FMT_MTD.1/AdminAct, FMT_SMF.1)

4 Security Requirements

This section specifies a Security Functional Requirement for the TOE, as well as specifying the assurance activities the evaluator performs.

4.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated by the word "Refinement" in **bold text** after the element number with additional text in **bold** text and deletions with strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

If the EP specifies one or more iterations beginning with (2) (e.g. FTP_ITC.1(2) and FTP_ITC.1(3), it is because the same SFR is defined in the NDcPP but the EP requires one or more additional iterations of it in order to describe the TSF. In cases like this, the ST author is expected to add an iteration of (1) to the SFR that is defined in the NDcPP in order for the iteration convention to be consistent.

In cases where CC Part 2 specifies an assignment or selection operation and the PP has already completed the operation such that the ST author does not have the ability to perform this operation, the operation is indicated using the conventions described above but without any prompt to the ST author indicating "Selection:" or "Assignment:".

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

4.2 NDcPP Security Functional Requirement Direction

This section instructs the ST author what selections must be made to certain SFRs contained in the NDcPP in order to support related SFRs in the VPN Gateway PP. This is captured by expressing the element where the mandatory selection has been made. The ST author may complete the remaining selection items as they wish. To ensure specific capabilities or behavior is present in the TOE, selections in SFR elements have been made as well. In addition to providing the necessary selection required, there is an element, FPT_TST_EXT.1.2 that must be added to the NDcPP FPT_TST_EXT.1 component to be compliant with this EP.

The assurance activities for each SFR taken from the NDcPP are to be completed as they are defined in the Supporting Documents for that PP unless specifically indicated in this EP.

Note that for several of the requirements, only certain individual elements within the SFR have been changed for this EP. Any SFR elements that were omitted from the sections below are to be included in a conformant ST unmodified from their definition in the NDcPP.

4.2.1 FAU_GEN.1 Audit Data Generation

There are no additional SFRs for security audit defined by this EP. However, there are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the NDcPP. As such, the following events should be combined with those of the NDcPP in the context of a conforming Security Target.

4-1 FAU_GEN.1 Audit Event and Details

Requirement	Auditable Events	Additional Audit Record Contents
FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment
FIA_X509_EXT.1	Session establishment with CA	Entire packet contents of packets transmitted/received during session establishment
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets

Application Note: *For session establishment, the expectation is that the TOE is capable of auditing all of the packets associated with the establishment of a session; this would include the IKE phase 1 and phase 2 negotiations. The TOE must be able to log all of the packets in a successful session establishment, and also have the ability to log any packets that were dropped or discarded.*

Activity	Assurance Activity
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 should have been addressed with a combination of the TSS assurance 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.
AGD	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 should have been addressed with a combination of the guidance assurance 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 this EP. 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

Activity	Assurance Activity
	records that it is unable to process all of the received packets.

4.2.2 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) Refinement: The TSF shall perform *encryption/ decryption* in accordance with a specified cryptographic algorithm *AES operating in GCM, CBC* and cryptographic key sizes **128 bits, 256 bits, and [selection: 192 bits, no other key sizes]** that meet the following: *AES as specified in ISO 18033-3, CBC as specified in ISO 10116, GCM as specified in ISO 19772*.

Application Note: *This SFR has been modified from its definition in the NDcPP by mandating both GCM and CBC modes as well as both 128 and 256 bit key sizes at a minimum.*

4.2.3 FCS_IPSEC_EXT.1 Extended: IPsec

This EP modifies this NDcPP SFR for IPsec by including some refinements that apply specifically to products that implement IPsec as a VPN Gateway. It is also included here because this EP mandates its inclusion whereas the NDcPP defines it as an optional requirement.

FCS_IPSEC_EXT.1.3 Refinement: The TSF shall implement transport mode and **[selection: tunnel mode, no other mode]**.

Application Note: *Future versions of this EP will require that the TSF implement both tunnel mode and transport mode.*

FCS_IPSEC_EXT.1.4 Refinement: The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602) and **AES-GCM-128 (specified in RFC 4106), AES-GCM-256 (specified in RFC 4106)** together with a Secure Hash Algorithm (SHA)-based HMAC.

FCS_IPSEC_EXT.1.11 Refinement: The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), **19 (256-bit Random ECP), 20 (384-bit Random ECP),** and [selection: 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS), ~~20 (384-bit Random ECP),~~ no other DH groups].

4.2.4 FMT_MOF.1/AdminAct Management of Security Functions Behavior

This SFR is defined in the NDcPP as optional but is mandated for inclusion in this EP. Note that while the text of the SFR is unchanged from its definition in the NDcPP, its inclusion in an ST that is conformant with this EP means that "TOE Security Functions" should be understood to include the functionality specified in this EP as well as any relevant functionality that is defined by the base NDcPP.

4.2.5 FMT_MTD.1/AdminAct Management of TSF Data

This EP modifies this NDcPP SFR for TSF data storage by including certificates in the set of data to be managed securely. It is also included here because the SIP Server EP mandates its inclusion whereas the NDcPP defines it as an optional requirement.

FMT_MTD.1.1/AdminAct Refinement: The TSF shall restrict the ability to *modify, delete, generate/import* the *cryptographic keys* ***and certificates used for VPN operation*** to *Security Administrators*.

4.2.6 FMT_SMF.1 Specification of Management Functions

Additional management functions extend the FMT_SMF.1 SFR found in the NDcPP. The following functions shall be combined with those of the NDcPP in the context of a conforming Security Target.

- *Ability to configure the cryptographic functionality,*
- *Ability to configure the IPsec functionality,*
- *Ability to import X.509v3 certificates,*
- *Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE identified in this EP to the Administrator,*
- *Ability to configure all security management functions identified in other sections of this EP.*

Application Note: *In order to prevent redundancy, an ST claiming conformance to this EP should not select "Ability to configure the cryptographic functionality" as defined in the NDcPP when completing FMT_SMF.1 since it is already mandated by this EP.*

The following assurance activity is to be performed in addition to the assurance activities specified by the NDcPP Supporting Documents for this SFR.

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS describes how the traffic filter rules can be configured. Note that this activity should have been addressed with the TSS assurance activities for FPF_RUL_EXT.1.
AGD	The evaluator shall verify that the operational guidance describes how to configure the traffic filter rules, including how to set any configurable defaults and how to configure each of the applicable rule attributes, actions, and associated interfaces. The evaluator must ensure that the operational guidance also provides instruction that would allow an administrator to ensure that configured rules are properly ordered. Note that this activity should have been addressed with the Guidance assurance activities for FPF_RUL_EXT.1.
Test	The evaluator shall devise tests that demonstrate that the functions used to configure the TSF yield expected changes in the rules and that they are correctly enforced. A number of rule combination and ordering scenarios need to be configured and tested by attempting to pass both valid and invalid network traffic through the TOE. Note that this activity should have been addressed with a combination of the Test assurance activities for FPF_RUL_EXT.1

4.2.7 FPT_TST_EXT.1 Extended: TSF Testing

FPT_TST_EXT.1.2 The TSF shall provide the capability to verify the integrity of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1(2).

Application Note*: The NDcPP contains one element for this component, which simply requires a suite of self-tests to demonstrate correct operation of the TSF. This element is added to that component to further mitigate the threat of insecure operations.*

4.2.8 FPT_TUD_EXT.1 Extended: Trusted Update

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

Application Note: *The NDcPP provides an option of which method of verification the ST author wishes to specify. For compliance with this EP, a digital signature mechanism (one of those specified in FCS_COP.1(2) must be employed. Note that the ST author should include the other two elements of the*

NDcPP FPT_TUD_EXT.1 in the ST without modification. This may also trigger the inclusion of the NDcPP's selection-based SFR FPT_TUD_EXT.2 as specified in the NDcPP if "code signing for system software updates" is selected in FIA_X509_EXT.2 of the NDcPP..

4.2.9 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall use **IPsec, and [selection: SSH, TLS, TLS/HTTPS, no other protocols]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, VPN communications, [selection: authentication server, [*assignment: other capabilities*], no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

***Application Note**: The NDcPP allows trusted channels other than IPsec to be available for communication with external IT entities but defers to this EP to specify VPN Gateway functionality. To be compliant with this EP, the selection is made such that the TOE must provide the IPsec protocol for its VPN Gateway functionality. Protection (by at least one of the listed protocols) is required at least for communications with the server that collects the audit information (per the NDcPP). For communication with any other authorized IT entity, the ST author makes the appropriate selections/assignments and includes the related requirements from Annex C corresponding to their selections.*

4.3 TOE Security Functional Requirements

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

FCS_CKM.1.1/IKE Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a:

[selection, choose at least one of:

- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes;**
- **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves];**
- **ANSI X9.31-1998, Section 4.1 Using AES for RSA schemes**

]

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

***Application Note**: The ANSI X9.31-1998 option will be removed from the selection in a future publication of this document. Presently, the selection is not exclusively limited to the FIPS PUB 186-4 options in order to allow industry some further time to complete the transition to the modern FIPS PUB 186-4 standard.*

The keys that are required to be generated by the TOE through this requirement are intended to be used for the authentication of the VPN peers during the IKE (either v1 or v2) key exchange. While it is required that the public key be associated with an identity in an X509v3 certificate, this association is not required to be performed by the TOE, and instead is expected to be performed by a Certificate Authority in the Operational Environment.

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

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

Activity	Assurance Activity
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.
AGD	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	The evaluator shall use the key pair generation portions of "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)" and "The RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

4.3.2 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 Refinement: The TSF shall detect when **an Administrator configurable positive integer of successive** unsuccessful authentication attempts occur related to **administrators attempting to authenticate remotely**.

FIA_AFL.1.2 Refinement: When the defined number of unsuccessful authentication attempts has been met, the TSF shall **[selection, choose one of: prevent the offending remote administrator from successfully authenticating until [*assignment: action*] is taken by a local Administrator; prevent the offending remote administrator from successfully authenticating until an Administrator defined time period has elapsed]**.

***Application Note**: This requirement does not apply to an administrator at the local console, since it does not make sense to lock a local administrator’s account in this fashion. This could be addressed by (for example) requiring a separate account for local administrators or having the authentication mechanism implementation distinguish local and remote login attempts. The “action” taken by a local administrator is implementation specific and would be defined in the administrator guidance (for example, lockout reset or password reset). The ST author chooses one of the selections for handling of authentication failures depending on how the TOE has implemented this handler.*

Activity	Assurance Activity
TSS	The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful

Activity	Assurance Activity
	authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.
AGD	The evaluator shall also examine the operational guidance to ensure that instructions for configuring the number of successive unsuccessful authentication attempts (FIA_AFL.1.1) and time period (FIA_AFL.1.2, if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
Test	The evaluator shall perform the following tests for IPsec, and for each other method by which remote administrators access the TOE (e.g., TLS, SSH): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached, attempts with valid credentials are not successful. For each action specified by the requirement, the evaluator shall show that following the operational guidance and performing each action to allow the remote administrator access are successful. Test 2: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE and a time period after which valid logins will be allowed for a remote administrator. After exceeding the specified number of invalid login attempts and showing that valid login is not possible, the evaluator shall show that waiting for the interval defined by the time period before another access attempt will result in the ability for the remote administrator to successfully log on using valid credentials.

4.3.3 FIA_X509_EXT.4 X.509 Certificate Identity

FIA_X509_EXT.4.1 The TSF shall not establish an SA if the distinguished name (DN) contained in a certificate does not match the expected DN for the entity attempting to establish a connection.

Activity	Assurance Activity
TSS	The TSS shall describe all certificate stores implemented that contain certificates used to meet the requirements of this EP. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access. The TSS description will also include a discussion as to how the TOE forms a certification path as specified in the standard and how certificates are validated (CRL and/or OCSP are included in the discussion, as well as the certificate path validation algorithm).
AGD	The evaluator shall verify that the operational guidance describes how to configure the TOE to either allow or disallow the establishment of an SA.
Test	This SFR is tested as part of FCS_IPSEC_EXT.1 as defined by the NDcPP.

4.3.4 FPF_RUL_EXT.1 Packet Filtering

FPF_RUL_EXT.1.1 The TSF shall perform Packet Filtering on network packets processed by the TOE.

Activity	Assurance Activity
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.
AGD	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
Test	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 directed at the TOE's interfaces, with packet sniffers listening to see if any network traffic is allowed through. Note: The remaining testing associated with application of the ruleset is addressed in the subsequent test assurance activities.

FPF_RUL_EXT.1.2 The TSF shall process the following network traffic protocols:

- Internet Protocol (IPv4)
- Internet Protocol version 6 (IPv6)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

and be capable of inspecting network packet header fields defined by the following RFCs to the extent mandated in the other elements of this SFR

- RFC 791 (IPv4)
- RFC 2460 (IPv6)
- RFC 793 (TCP)
- RFC 768 (UDP).

Application Note: *This element identifies the protocols and references the protocol definitions that serve to define to what extent the network traffic can be interpreted by the TOE when importing (receiving network traffic or ingress) and exporting (sending – or forming to be sent - network traffic or egress).*

While the protocol formatting specified in the RFCs is still used, many RFCs define behaviors which are no longer considered safe to follow. For example, RFC792 defined the "Redirect" ICMP type, which is not considered safe to honor when it might come from an adversary; the "source quench" message, which is insecure because its source cannot be validated.

Activity	Assurance Activity
TSS	The evaluator shall verify that the TSS indicates that the following protocols are

Activity	Assurance Activity
	supported: • RFC 791 (IPv4) • RFC 2460 (IPv6) • RFC 793 (TCP) • RFC 768 (UDP) 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).
AGD	The evaluator shall verify that the operational guidance indicates that the following protocols are supported: • RFC 791 (IPv4) • RFC 2460 (IPv6) • RFC 793 (TCP) • RFC 768 (UDP) The guidance will 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 ensures it is made clear what protocols were not considered as part of the TOE evaluation.
Test	The testing associated with this requirement is addressed in the subsequent test assurance activities.

FPF_RUL_EXT.1.3 The TSF shall allow the definition of Packet Filtering rules using the following network protocol fields:

- IPv4
  - Source address
  - Destination Address
  - Protocol
- IPv6
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

and distinct interface.

Application Note: *This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement – the applicable interface is a property of the TOE and the rest of the identified attributes are defined in the associated RFCs. Note that the Protocol is the IPv4 field (in IPv6 this field is called the "next header") that identifies the applicable protocol, such as TCP, UDP, ICMP, etc. Also, 'Interface' identified above is the external port where the applicable network traffic was received or alternately will be sent.*

FPF_RUL_EXT.1.4 Refinement: The TSF shall allow the following operations to be associated with Packet Traffic Filtering rules: permit, ~~deny~~, **discard,** and log.

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

FPF_RUL_EXT.1.5 The TSF shall allow the Packet Traffic Filtering rules to be assigned to each distinct network interface.

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

Note that there could be a separate ruleset for each interface or alternately a shared ruleset that somehow associates rules with specific interfaces.

Activity	Assurance Activity

TSS	The evaluator shall verify that the TSS describes a Packet Filtering policy and the following attributes are:
	• IPv4
	  ○ Source address
	  ○ Destination Address
	  ○ Protocol
	• IPv6
	  ○ Source address
	  ○ Destination Address
	  ○ Next Header (Protocol)
	• TCP
	  ○ Source Port
	  ○ Destination Port
	• UDP
	  ○ Source Port
	  ○ Destination Port
	The evaluator shall verify that each rule can identify the following actions: permit, deny, 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.

AGD	The evaluators shall verify that the operational guidance identifies the following attributes as being configurable within Packet filtering rules for the associated protocols:

Activity	Assurance Activity

	• IPv4
	  ○ Source address
	  ○ Destination Address
	  ○ Protocol
	• IPv6
	  ○ Source address
	  ○ Destination Address
	  ○ Next Header (Protocol)
	• TCP
	  ○ Source Port
	  ○ Destination Port
	• UDP
	  ○ Source Port
	  ○ Destination Port
	
	The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, deny, and log.
	
	The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces.

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, deny, 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: Repeat the test assurance activity above to ensure that Packet filtering rules can be defined for each distinct network interface type supported by the TOE.
	
	Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.7 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.1.7 define the

Activity	Assurance Activity
	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.1.6 The TSF shall process the applicable Packet Filtering rules (as determined in accordance with FPF_RUL_EXT.1.5) in the following order: Administrator-defined.

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

Activity	Assurance Activity
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.
AGD	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 deny. 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.1.7 The TSF shall drop traffic if a matching rule is not identified.

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

Activity	Assurance Activity
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 deny packets when there is no rule match unless another required conditions allows the network traffic (i.e., FPF_RUL_EXT.1.6 or FPF_RUL_EXT.1.7).
AGD	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 deny 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

Activity	Assurance Activity
	Transport Layer Protocol (see table **Error! Reference source not found.**) 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 deny and log each defined IPv4 Transport Layer Protocol (see table **Error! Reference source not found.**) 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 **Error! Reference source not found.**) 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 deny and log each defined IPv4 Transport Layer Protocol (see table **Error! Reference source not found.**) 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). Test 4: The evaluator shall configure the TOE to permit and log each defined IPv6 Transport Layer Protocol (see table **Error! Reference source not found.**) 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 deny and log each defined IPv6 Transport Layer Protocol (see table **Error! Reference source not found.**) 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

Activity	Assurance Activity
	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 **Error! Reference source not found.**) 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 deny and log each defined IPv6 Transport Layer Protocol (see table **Error! Reference source not found.**) 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 deny 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 deny 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.

4.3.5 FPT_FLS.1/SelfTest Fail Secure

FPT_FLS.1.1/SelfTest Refinement: The TSF shall **shut down** when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

Application Note: *The failures relevant to this requirement are the FPT_TST_EXT.1.1 requirement in the NDcPP, and the FPT_TST_EXT.1.2 requirement specified in this EP.*

Activity	Assurance Activity
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, those cases are identified and a rationale supporting the classification and justification why the TOE's ability to enforce its security policies is not affected.
AGD	There are no operational guidance activities for this requirement.
Test	There are no test activities for this requirement.

5 Security Assurance Requirements

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDcPP as well. The NDcPP includes a number of Assurance Activities associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this EP includes a number of SFR-based Assurance Activities that similarly refine the SARs associated with the EAL identified in the NDcPP. The assurance activities associated with SARs that are prescribed by the NDcPP are performed against the entire TOE, with the addition of the specific vulnerability testing described here.

5.1.1 AVA_VAN.1 Vulnerability survey

The evaluator shall generate network packets that cycle through all of the values for attributes, Type, Code, and Transport Layer Protocol, that are undefined by the RFC for each of the protocols, ICMPv4, ICMPv6, IPv4, and IPv6. For example, ICMPv4 has an eight-byte field for Type and an eight-byte field for the Code. Only 21 Types are defined in the RFC (see table E-1), but there are 256 possible value. Each Type has a Code associated with it, the number of RFC defined Codes varies based on the Type. The evaluator is required to construct packets that exercise each possible value not defined in the RFC (the defined values are already tested in FPF_RUL_EXT.1.10) of Type and Code (including all possible combinations) and target each distinct interface type to determine that the TOE handles these packets appropriately. Since none of these packets will match a rule, or belong to an allowed session the packets should be discarded. Since there are no requirements that the TOE audit a packet being discarded under these circumstances, the evaluator shall ensure the TOE does not allow these packets to flow through the TOE.

In addition to the undefined attribute testing required above, the evaluator shall perform intelligent fuzz testing of the remaining fields in the required protocol headers (excluding FTP). The intent of intelligent fuzzing is that a packet that is otherwise correctly constructed, such that it will be denied when the ruleset is applied, has random values inserted into each of the protocol header fields. The evaluator ensures a statistically significant sample size, which will vary depending on the protocol field length, is used and is justified in their report.

The evaluator should consult whatever diagnostics (e.g., logging, process status, interface errors) the TOE offers to determine if the TOE was adversely impacted by the processing of such packets.

Appendix A: Rationale

In this EP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats addressed by IPsec VPN Gateways; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this section contains the tabular artifacts that can be used for the evaluation activities associated with this document.

A.1 Security Problem Definition

A.1.1 Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions are in addition to those defined in the NDcPP and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

A-1 TOE Assumptions

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

A.1.2 Threats

The threats listed below are addressed by VPN Gateways. Note that these threats are in addition to those defined in the NDcPP, all of which apply to VPN Gateways.

A-2 Threats

Threat Name	Threat Definition
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T. NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to Operational Environment policies.
T.TSF_FAILURE	Security mechanisms of the TOE mail fail, leading to a compromise of the TSF.
T.REPLAY_ATTACK	If malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.
T.DATA_INTEGRITY	A malicious party attempts to change the data being sent – resulting in loss of integrity.

A.1.3 Organizational Security Policies

No organizational policies have been identified that are specific to VPN Gateways. However, all the organizational security policies in the NDcPP apply to VPN Gateways.

A.1.4 Security Problem Definition Correspondence

The following table serves to map the threats and assumptions defined in this EP to the security objectives also defined or identified in this EP.

A-3 Security Problem Definition Correspondence

Threat or Assumption	Security Objectives
A.CONNECTIONS	OE.CONNECTIONS
T.NETWORK_DISCLOSURE	O.ADDRESS_FILTERING and O.PORT_FILTERING
T. NETWORK_ACCESS	O.ADDRESS_FILTERING, O.RELATED_CONNECTION_FILTERING, and O.PORT_FILTERING
T.NETWORK_MISUSE	O.ADDRESS_FILTERING, O.PORT_FILTERING, and O.SYSTEM_MONITORING
T.TSF_FAILURE	O.FAIL_SECURE
T.REPLAY_ATTACK	O.CRYPTOGRAPHIC_FUNCTIONS
T.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS

A.2 Security Objectives

A.2.1 Security Objectives for the TOE

The following table contains security objectives for the TOE. A TOE that conforms to this shall be capable of satisfying these security objectives.

A-4 Security Objectives for the TOE

Security Objective Name	Security Objective Definition
O.ADDRESS_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination addresses.
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE
O.FAIL_SECURE	Upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
O.PORT_FILTERING	The TOE will provide the means to filter and log network packets based on source and destination transport layer ports.

A.2.2 Security Objectives for the Operational Environment

The following table contains security objectives specific to the operational environments for VPN Gateways. These security objectives are in addition to those defined in the NDcPP, all of which apply to the operational environments for VPN Gateways.

A-5 Security Objectives for the Operational Environment

Security Objective Name	Security Objective Definition
OE.CONNECTIONS	TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on network traffic flowing among attached networks.

A.2.3 Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.

Appendix B: Optional Requirements

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

B.1 Security Problem Description

In addition to the threats identified for the VPN gateway in a peer-to-peer multisite environment, there are unique concerns that are worrisome in the VPN headend configuration.

B.2 Threats

B.2.1 Unauthorized Client Connections

While a VPN client may have the necessary credentials (e.g., certificate, pre-shared key) to connect to a VPN gateway, there may be instances where the remote client, or the machine the client is operating on, has been compromised and attempts to make unauthorized connections.

(T.UNAUTHORIZED_CONNECTION)

B.2.2 Hijacked Session

There may be an instance where a remote client's session is hijacked due to session activity. This could be accomplished because a user has walked away from the machine that was used to establish the session.

(T.HIJACKED_SESSION)

B.2.3 Unprotected Client Traffic

A remote machine's network traffic may be exposed to a hostile network. A user may be required to use a hostile (or unknown) network to send network traffic without being able to route the traffic appropriately.

(T.UNPROTECTED_TRAFFIC)

B.3 Objectives

B.3.1 Client Establishment Constraints

To address the concern that a remote client may be compromised and attempt to establish connections with the headend VPN gateway outside of "normal" operations, this objective specifies conditions under which a remote client may establish connections. The administrator may configure the headend VPN gateway to accept a client's request for a connection based on attributes the administrator feels are appropriate.

(O.CLIENT_ESTABLISHMENT_CONSTRAINTS → FTA_TSE.1)

B.3.2 Remote Session Termination

A remote client's session can become vulnerability when there is a lack of activity. This is primarily due to a user walking away from a device that has a remote connection established. While some devices have a "lock screen" or logout capability, they cannot always assumed to be configured or available. To address this concern, a session termination capability is necessary during an administrator specified time period.

(O.REMOTE_SESSION_TERMINATION → FTA_SSL.3)

B.3.3 Assigned Private Address

There are instances where a remote client desires secure communication with a gateway that is trusted. While a user may be connected via an untrusted network, it should still be possible to ensure that it can communicate with a known entity that controls the routing of the client's network packets. This can be accomplished by the VPN headend assigning an IP address that the gateway controls, as well as providing a routing point for the client's network traffic.

(O.ASSIGNED_PRIVATE_ADDRESS → FTA_VCM_EXT.1)

B.4 FTA: TOE Access

These requirements specify how the TOE supports the establishment of sessions from VPN clients.

B.4.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 Refinement: The TSF shall terminate **a remote VPN client** session after an *Administrator-configurable time interval of session inactivity*.

Application Note: *This requirement exists in the NDcPP, however it is intended to address a remote administrative interactive session. Here, the requirement applies to a VPN client that has established a SA. After some configurable time period without any activity, the connection between the VPN headend and client is terminated. If the ST author is including the requirements for a VPN headend in their ST, this requirement should be iterated along with the requirement in the NDcPP.*

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

Activity	Assurance Activity
	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.

B.4.2 FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 Refinement: The TSF shall be able to deny establishment of a **remote VPN client** session based on *location, time, day, [selection: no other attributes, [assignment: other attributes]]*.

Application Note: *For this EP, location is defined as the client's IP address.*

Activity	Assurance Activity
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.
AGD	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.

B.4.3 FTA_VCM_EXT.1 VPN Client Management

FTA_VCM_EXT.1.1 The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

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

Activity	Assurance Activity
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.
AGD	There are no operational guidance activities for this requirement.
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.

Appendix C: Selection-Based Requirements

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

C.1.1 Pre-Shared Key Composition (FIA_PSK_EXT)

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

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

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

The requirements below allow the ST author to include these requirements in the ST, if they select pre-shared keys in the FCS_IPSEC_EXT.1.13 element defined in the NDcPP.

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

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

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

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

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

Activity	Assurance Activity
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.
AGD	The evaluator shall examine the operational guidance to determine that it provides

Activity	Assurance Activity
	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.
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.

Appendix D: Objective Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. There are additional requirements that specify security functionality that is desirable and these requirements are contained in this Appendix. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this EP.

At this time no objective requirements specific to this product type have been identified.

Appendix E: Transport Layer Protocols

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.

E-1 Defined Protocol-Specific Values

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

Protocol	Defined Attributes
	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