Network Device Protection Profile (NDPP) Extended Package
VPN Gateway

Information Assurance Directorate

12 April 2013

Version 1.1

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 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 *Security Requirements for Network Devices* protection profile (NDPP). 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 NDPP.

1.1 Conformance Claims

The *Security Requirements for Network Devices* Protection Profile (NDPP) defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP serves to extend the NDPP 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 NDPP, it is expected that the content of both this EP and the NDPP 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 NDPP (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 NDPP, conformant TOEs are obligated to implement the functionality required in the NDPP 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 rules are defined to control 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 NDPP, though they all apply given the conformance and hence dependence of this EP on the NDPP. Note also that while the NDPP 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 NDPP 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 Stateful Traffic Filter Firewall 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.

(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. The description of that security objectives are in addition to that described in [NDPP].

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_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.

(O.FAIL_SECURE → FPT_FLS.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, this security objective, which originated in the NDPP, is extended as follows.

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

To address the issues involved with a trusted means of administration of the VPN gateway, this security objective, which originated in the NDPP, is extended as follows. *Note that it is assumed that use of the functions indicated below is protected in accordance with the requirements in the NDPP.*

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 → FMT_SMF.1, FIA_AFL.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

While the SFR in this EP is extended, it is defined in a flexible manner for use in this and other EPs, or PPs, and as such operations are performed in the context of this EP.

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 EP author: Indicated with bold text and strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with italicized and underlined text; and
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

4.2 TOE Security Functional Requirements

There are eight SFR components that exist in the NDPP that required some form of modification in this EP. There are seven newly introduced SFRs contained in this EP, and three audit events were specified as well.

4.2.1 NDPP Security Functional Requirement Direction

This section instructs the ST Author what selections must be made to certain SFRs contained in the NDPP 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 NDPP FPT_TST_EXT.1 component to be compliant with this EP.

Assurance activities are not repeated for the requirements in this section, as those are already captured in the NDPP. What is important for the evaluator when they assess the ST and TOE against the SFRs as specified here is that the proper selections have been made and the appropriate tests are performed to demonstrate compliance to the requirements.

4.2.1.1 FCS_CKM.1(1) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1 Refinement: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard"*
- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*

- [selection: *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes,* no other]

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

Application Note: This EP requires specific algorithms to be used in key establishment, and this instantiation of the requirement from the NDPP ensures the right selections are made.

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

FCS_COP.1.1(1) **Refinement:** The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm *AES operating in* **GCM, CBC,** [**assignment: *one or more modes, no other modes***]] and cryptographic key sizes 128-bits, 256-bits, and [**selection: 192 bits, no other key sizes**] that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **NIST SP 800-38D, NIST SP 800-38A [selection:, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38E, no other standards]**

Application Note: This EP requires the modes GCM and CBC to be used in the IPsec and IKE protocols (FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6). Therefore, the FCS_COP.1.1(1) element in the NDPP has been specified here to ensure the ST Author includes these two modes to be consistent with the IPsec requirements.

4.2.1.3 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a:

- **[selection, choose at least one of: *RSA Digital Signature Algorithm (RSA) with a key size (modulus) of 2048 bits or greater that meets* FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard",**
- ***Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater] that meets* FIPS PUB 186-3, "Digital Signature Standard" with "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")].**

4.2.1.4 FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Appendix C; X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source, and [selection: a software-based noise source, other independent TSF-hardware-based noise source, no other noise source].

Application Note: The NDPP allows the ST Author to choose whether the noise source is software based or hardware based. For compliance with this EP, there must be at least one hardware based noise source.

A hardware noise source is a component that produces data that cannot be explained by a deterministic rule, due to its physical nature. In other words, a hardware based noise source generates sequences of random numbers from a physical process that cannot be predicted. For example, a sampled ring oscillator consists of an odd number of inverter gates chained into a loop, with an electrical pulse traveling from inverter to inverter around the loop. The inverters are not clocked, so the precise time required for a complete circuit around the loop varies slightly as various physical effects modify the small delay time at each inverter on the line to the next inverter. This variance results in an approximate natural frequency that contains drift and jitter over time. The output of the ring oscillator consists of the oscillating binary value sampled at a constant rate from one of the inverters – a rate that is significantly slower than the oscillator's natural frequency.

Any hardware component behaving in similarly variable ways that cannot be explained by a precise and predictable rule can serve as a hardware-based noise source. It is also possible to use multiple independent noise sources to increase entropy production and reduce attack potential (by requiring attackers to exploit multiple random bit streams) as long as at least one of the sources is hardware based. It should be noted that timing of interrupts caused by mechanical I/O devices and system counters are not considered *hardware-based* noise sources for the purposes of this requirement.

See Appendix D of the NDPP for further explanation regarding entropy.

4.2.1.5 FMT_SMF.1 Specification of Management Functions

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

- *Ability to configure the cryptographic functionality,*
- *Ability to configure the IPsec functionality,*
- 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.*

4.2.1.6 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify 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 NDPP 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.

4.2.1.7 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 all authorized IT entities 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 NDPP allows trusted channels other than IPsec to be available for communication with external IT entities. To be compliant with this EP, the selection is made such that the TOE must provide the IPsec protocol as a configurable option to the administrator.

4.2.1.8 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 NDPP 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 comply with the EP.

4.2.2 FCS_CKM.1 (2) Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.2 **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 186-3, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA schemes;
- FIPS PUB 186-3, “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, Appendix A.2.4 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 186-3 options in order to allow industry some further time to complete the transition to the modern FIPS PUB 186-3 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.

4.2.3 FCS_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications

The set of the IPsec requirements specified here take precedent over the IPsec requirements specified in the NDPP.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection, choose at least one of: tunnel mode, transport mode].

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

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

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

Application Note: If an AES-CBC selection is made, the SHA-based HMAC must be consistent with what is specified in the NDPP FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication) requirement.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, [selection: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers] and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23) and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection, choose at least one of: IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 6379 and [selection: AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

Application Note: Element 1.7 is only applicable if IKEv1 is selected.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: IKEv2 SA lifetimes can be configured by an Administrator based on number of packets or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs, IKEv1 SA lifetimes can be configured by an Administrator based on number of packets or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs].

Application Note: It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment: (one or more) number(s) of bits that is at least twice the "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, *Recommendation for Key Management – Part 1: General*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[assignment: (one or more) "bits of security" value(s) associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, *Recommendation for Key Management – Part 1: General*] .

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

FCS_IPSEC_EXT.1.12 The TSF shall ensure that all IKE protocols perform peer authentication using a [selection, choose at least one of: *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre-shared Keys, no other method].

FCS_IPSEC_EXT.1.13 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [selection: IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

4.2.4 FPF_RUL_EXT.1 Packet Filtering

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

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.

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

Application Note: This element defines the operations that can be associated with rules used to match network traffic. Note that the data to be logged is identified in the Security Audit requirements, see Section 4.2.9.

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.

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.

FPF_RUL_EXT.1.7 The TSF shall deny packet flow 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.

Authentication Failure Handling (FIA_AFL)

4.2.5 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 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.

4.2.6 FIA_X509_EXT.1 Extended: X.509 Certificates

FIA_X509_EXT.1.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [selection: no other protocols, TLS, SSH] connections.

FIA_X509_EXT.1.2 The TSF shall store and protect certificate(s) from unauthorized deletion and modification.

FIA_X509_EXT.1.3 The TSF shall provide the capability for authenticated Administrators to load X.509v3 certificates into the TOE for use by the security functions specified in this PP.

FIA_X509_EXT.1.4 The TSF shall generate a Certificate Request Message as specified in RFC 2986 and be able to provide the following information in the request: public key, Common Name, Organization, Organizational Unit, and Country.

Application Note: The public key referenced in FIA_X509_EXT.1.4 is the public key portion of the public-private key pair generated by the TOE as specified in FCS_CKM.1(2).

FIA_X509_EXT.1.5 The TSF shall validate the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].

Application Note: While the choice of revocation method employed is left to the ST author, future versions of this EP will mandate both methods be available to the TOE's Administrator.

FIA_X509_EXT.1.6 The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.

FIA_X509_EXT.1.7 The TSF shall not treat a certificate as a CA certificate if the basicConstraints extension is not present or the cA flag is not set to TRUE.

FIA_X509_EXT.1.8 The TSF shall not establish an SA if a certificate or certificate path is deemed invalid.

FIA_X509_EXT.1.9 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.

FIA_X509_EXT.1.10 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall, at the option of the administrator, establish an SA or disallow the establishment of an SA.

Application Note: The intent of FIA_X509_EXT.1.8 is that the TOE is configurable to allow or disallow session establishment if the TOE cannot connect to an entity responsible for providing certificate validation information. For instance, if a CRL cannot be obtained because a machine is down, or the network path is broken, the administrator may elect to configure the TOE to allow sessions to continue

to be established, rather than terminate the TOE's ability to establish any new SAs because it cannot reach the CA.

4.2.7 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 **Refinement**: The TSF shall restrict the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE identified in this EP to an authenticated Administrator.

4.2.8 FPT_FLS.1 Fail Secure

FPT_FLS.1.1 **Refinement:** The TSF shall **shutdown** 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 NDPP, and the FPT_TST_EXT.1.2 requirement specified in this EP.

4.2.9 Security Audit

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

The following audit events are required for this EP.

4-1 FAU_GEN.1 Audit Event and Details

Requirement	Auditable Events	Additional Audit Record Contents
FCS_IPSEC_EXT.1	Session Establishment with peer	Source and destination addresses Source and destination ports TOE Interface
FIA_X509_EXT.1	Establishing session with CA	Source and destination addresses Source and destination ports TOE Interface
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.

5 Assurance Activities

This section contains the assurance activities associated with the SFRs contained within this EP. The assurance activities are grouped according to the CC component they are associated with.

The assurance activities are intended to address the required content of the TOE Summary Specification (TSS) of the ST, the required content of the TOE's operational guidance, and required test activities to be independently performed by the evaluators.

It is assumed the evaluator will have tools suitable to establish sessions, modify or create session packets, and perceive whether packets are getting through the TOE as well as to examine the content of those packets. In general, it is expected that Packet Filtering rule configuration and logging capabilities of the TOE can be used to reach appropriate determinations where applicable.

The tests specified below need to be repeated for each distinct network interface type. Given the definition of interface type (all packets are processed through the same logical path within the TOE) tests are necessary to ensure all logical paths that a packet may take through the TOE adhere to the security policy specified by this EP.

The evaluators shall minimally create a test environment equivalent to the test environment illustrated below. The evaluators must provide Justification for any differences in the test environment.

5.1.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1

TSS

1 In order to show that the TSF complies with 800-56A and 800-56B (as selected) depending on the selections made, the evaluator shall ensure that the TSS contains the following information:

- The TSS shall list all sections of the appropriate 800-56 standard(s) 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 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described;

Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.

Guidance

The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.

Test

The evaluator shall use the key pair generation portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-3 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.

FCS_CKM.1.2

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 186-3, the evaluator shall ensure that the TSS contains the following information:

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

Any TOE-specific extensions, processing that is not included in the Appendices, or alternative implementations allowed by the Appendices that may impact the security requirements the TOE is to enforce shall be described.

Guidance

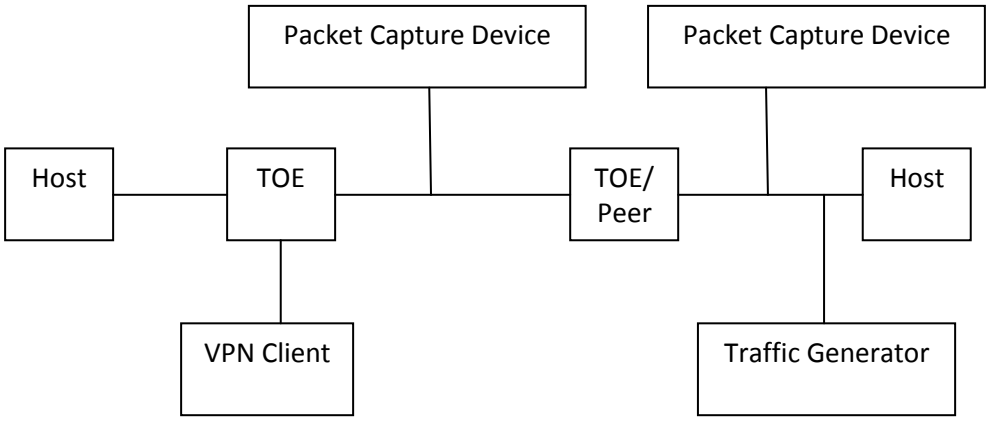
The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.

Test

The evaluator shall use the key pair generation portions of "The FIPS 186-3 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.

5.1.2 FCS_IPSEC_EXT.1 Extended: Internet Protocol Security (IPsec) Communications

In order to show that the TSF implements the RFCs correctly, the evaluator shall perform the assurance activities listed below. In future versions of this EP, assurance activities may be augmented, or new ones introduced that cover more aspects of RFC compliance than is currently described in this publication.



The evaluators shall minimally create a test environment equivalent to the test environment illustrated above. Two instantiations of the TOE will more than likely make it easier to conduct testing and if there is a failure of a test it should be more easily traced to the TOE, however, the evaluator is free to construct a testbed where one instance of a TOE exists and there is a device that provides the necessary functions to interact with the TOE to satisfy the testing activities. If the ST author includes the requirements for a VPN Headend, it is expected that a VPN client be used to demonstrate the TOE can act as a remote access VPN headend as well as the requirements specified for VPN client management. It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability manipulate fields in the IPv4, IPv6, UDP, and TCP packet headers. The evaluators must provide Justification for any differences in the test environment. One such justification may be that the host can implement a traffic generator. It would be more difficult to make the same argument for the packet capture device, since it is expected the evaluator will have access to packets that are actually on the wire.

FCS_IPSEC_EXT.1.1

TSS

Nothing is done in addition to determining that the TOE's implementation is conformant to RFC 4301 as described above.

Guidance

The evaluator shall examine the operational guidance to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for DISCARD, BYPASS and PROTECT.

Test

The evaluator uses the operational guidance to configure the TOE to carry out the following tests:

Test 1: The evaluator shall configure the TOE's SPD such that there is a rule for DISCARD, BYPASS, PROTECT. The selectors used in the construction of the rule shall be different such that the evaluator can send in three network packets with the appropriate fields in the packet header that each packet will match one of the three rules. The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packet was dropped, allowed through without modification, was encrypted by the IPsec implementation.

Test 2: The evaluator shall devise two equal SPD entries with alternate operations – BYPASS and PROTECT. The entries should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first entry is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.

Test 3: The evaluator shall repeat the procedure above, except that the two entries 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.

FCS_IPSEC_EXT.1.2

TSS

The evaluator checks the TSS to ensure it states that the TOE can operate in tunnel mode and/or transport mode (as selected).

Guidance

The evaluator shall confirm that the operational guidance instructs the Administrator how the TOE is configured in each mode selected.

Test

Test 1 (conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE in tunnel mode, and a TOE peer in tunnel mode. The evaluator configures the two peer TOEs to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a session between the peers. The evaluator observes in the audit trail and the captured packets that a successful connection was established using the tunnel mode.

Test 2 (conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode when it receives packets from the VPN client. The evaluator configures the TOE and VPN client to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection with the TOE using the VPN client. The evaluator observes in the audit trail and the captured packets that a successful connection was established using the transport mode.

FCS_IPSEC_EXT.1.3

TSS

The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no "rules" are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Guidance

The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.

Test

Test 1: The evaluator shall configure the TOE's SPD, such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator also configures the TOE so that all auditable events with respect to FCS_IPSEC_EXT.1 are enabled. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry, and send that packet to the TOE. The evaluator should observe that the network packet is passed by the TOE to the proper destined interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet to the TOE, and observes that the packet was not permitted to flow to any of the TOE's interfaces. The evaluator shall verify that an audit record is generated that specifies that the packet was discarded as expected.

FCS_IPSEC_EXT.1.4

TSS

The evaluator shall examine the TSS to verify that the algorithms AES-GCM-128 and AES-GCM-256 are implemented. If the ST author has selected either AES-CBC-128 or AES-CBC-256 in the requirement, then the evaluator verifies the TSS describes these as well. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(4) Cryptographic Operations (for keyed-hash message authentication).

Guidance

The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the AES-GCM-128, and AES-GCM-256 algorithms, and if either AES-CBC-128 or AES-CBC-256 have been selected the guidance instructs how to use these as well.

Test

Test 1: The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the AES-GCM-128, and AES-GCM-256 algorithms, and attempt to establish a connection using ESP in confidentiality and integrity mode. If the ST Author has selected either AES-CBC-128 or AES-CBC-256, the TOE is configured to use those algorithms and the evaluator attempts to establish a connection using ESP in confidentiality and integrity mode for those algorithms selected.

FCS_IPSEC_EXT.1.5

TSS

The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

Guidance

The evaluator checks the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test.

Test

Test 1: The evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.

FCS_IPSEC_EXT.1.6

TSS

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Guidance

The evaluator ensures that the operational guidance describes how the TOE can be configured to use the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test.

Test

Test 1: The evaluator shall configure the TOE to use AES-CBC-128 to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using AES-CBC-128. The evaluator will consult the audit trail to confirm the algorithm was that used in the negotiation.

FCS_IPSEC_EXT.1.7

TSS

The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.

Guidance

If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.

Test

Test 1 (conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.

FCS_IPSEC_EXT.1.8

TSS

How the lifetimes are established and enforced is described in the RFCs and the evaluator examines the TSS as stated at the beginning of this section.

Guidance

The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. The evaluator ensures that the Administrator is able to configurable Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no values mandated for the number of packers, the evaluator just ensures that this can be configured. The TOE may limit the lifetime on the number of bytes that have been transmitted and this would be acceptable.

Test

When testing this, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

Test 1: The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.

Test 2: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

Test 3: The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.

FCS_IPSEC_EXT.1.9, FCS_IPSEC_EXT.1.10

The evaluator shall check to ensure that, for each DH group supported by the TSF, the TSS describes the process for generating "x" (as defined in FCS_IPSEC_EXT.1.9) and each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

FCS_IPSEC_EXT.1.11

The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer. The evaluator shall also perform the following test*:*

Test 1: For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.

FCS_IPSEC_EXT.1.12

TSS

The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1(2) Cryptographic Operations (for cryptographic signature).

Guidance

The evaluator ensures the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA and/or ECDSA.

In order to construct the environment and configure the TOE for the following tests, the evaluator will ensure that the operation guidance also describes how to configure the TOE to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”.

Test

For efficiency sake, the testing that is performed here has been combined with aspects of the testing for FIA_X509_EXT.1 Extended: X.509 Certificates, specifically FIA_X509_EXT.1.4, and FIA_X509_EXT.1.5.

The following five tests shall be repeated for each peer authentication protocol selected in the FCS_IPSEC_EXT.1.12 selection above:

Test 1: The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request.

Test 2: The evaluator shall use a certificate signed using the RSA or ECDSA algorithm to authenticate the remote peer during the IKE exchange. This test ensures the remote peer has the certificate for the trusted CA that signed the TOE’s certificate and it will do a bit-wise comparison on the DN. This bit-wise comparison of the DN ensures that not only does the peer have a certificate signed by the trusted CA, but the certificate is from the DN that is expected. The evaluator will configure the TOE to associate a certificate (e.g., a certificate map in some implementations) with a VPN connection. This is what the DN is checked against.

Test 3: The evaluator shall test that the TOE can properly handle revoked certificates – conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this draft of the EP, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE will not establish an SA.

Test 4: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE’s certificate does not contain the basicConstraints extension. The validation of the certificate path fails.

Test 5: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE’s certificate has the cA flag in the basicConstraints extension not set. The validation of the certificate path fails.

Test 6: The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE’s certificate has the cA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.

Test 7: The evaluator shall test that given a signed certificate from a trusted CA, that when the DN does not match – any of the four fields can be modified such that they do not match the expected value, that an SA does not get established.

Test 8: The evaluator shall ensure that the TOE is configurable to either establish an SA, or not establish an SA if a connection to the certificate validation entity cannot be reached. For each method selected

for certificate validation, the evaluator attempts to validate the certificate – for the purposes of this test, it does not matter if the certificate is revoked or not. For the "mode" where an SA is allowed to be established, the connection is made. Where the SA is not to be established, the connection is refused.

FCS_IPSEC_EXT.1.13

TSS

The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.

Guidance

The evaluator simply follows the guidance to configure the TOE to perform the following tests.

Test

Test 1: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.

Test 2: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.

Test 3: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.

Test 4: This test shall be performed for each version of IKE supported by the TOE. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.

5.1.3 FPF_RUL_EXT.1 Extended: Packet Filtering

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.

Guidance

The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.

Tests

Test 1: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be 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

TSS

The evaluator shall verify that the TSS indicates that the following protocols are 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).

Guidance

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.

Tests

The testing associated with this requirement is addressed in the subsequent test assurance activities.

FPF_RUL_EXT.1.3/FPF_RUL_EXT.1.4/FPF_RUL_EXT.1.5

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.

Guidance

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

- 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.

The evaluator shall verify that the operational guidance explains how to determine the interface type of a distinct network interface (e.g., how to determine the device driver for a distinct network interface).

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 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

TSS

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

Guidance

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

Tests

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

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).

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 deny packets with no matching rules.

Tests

Test 1: The evaluator shall configure the TOE to permit and log each defined IPv4 Transport Layer Protocol (see table 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 9-1 Defined Protocol-specific Values) 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 denied (i.e., by capturing no applicable packets passing through the TOE).

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.

5.1.4 FIA_AFL.1 Authentication Failure Handling

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 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.

Guidance

The evaluator shall also examine the operational guidance to ensure that instructions for configuring the number of successive unsuccessful authentication attempts (1.1) and time period (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.

5.1.5 FIA_X509_EXT.1 Extended: X.509 Certificates

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).

Guidance

The evaluator shall verify that the operational guidance describes how to the administrator loads certificates into the certificate store. If the level of protection can managed by the administrator, the guidance provides a description of how to manage the protection mechanism. The guidance instructs the administrator how to generate a key pair and how to generate a Certificate Request Message to the CA.

The guidance documentation provides instructions how to select the method used for checking, as well as how to setup a protected communication path with the entity providing the information pertaining to certificate validity.

How the administrator can configure the TOE to either allow or disallow the establishment of an SA is also described in the operational guidance.

Test

The tests associated with this component are bundled with the FCS_IPSEC_EXT.1.12 requirements.

5.1.6 FMT_SMF.1 Specification of Management Functions

TSS

The evaluator shall verify that the TSS describes how the Packet filter firewall rules can be configured. Note that this activity should have been addressed with the TSS assurance activities for FPF_RUL_EXT.1.

Guidance

The evaluator shall verify that the operational guidance describes how to configure the Packet filter firewall 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

Test 1: The evaluator shall devise tests that demonstrate that the functions used to configure the Packet filter firewall rules yield expected changes in the rules 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.

5.1.7 FPT_FLS.1 Fail Secure FPT_FLS.1 Fail Secure

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.

5.1.8 FAU_GEN.1 Audit Event and Details

The following table defines the assurance activities to be performed by the evaluators in order to ensure conformance with FAU_GEN.1.

TSS

The evaluator shall verify that the TSS describes how the Packet filter firewall rules 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.

Guidance

The evaluator shall verify that the operational guidance describes how to configure the Packet filter firewall rules 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 to 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).

5.2 Security Assurance Requirements

It is important to note that a TOE that is evaluated against this EP is inherently evaluated against the NDPP as well. The NDPP 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 NDPP. The assurance activities associated with SARs that are prescribed by the NDPP are performed against the entire TOE, with the addition of the specific vulnerability testing described here.

5.2.1 AVA_VAN.1 Vulnerability survey

Assurance Activity:

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 4-2), 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 dropped. Since there are no requirements that the firewall audit a packet being dropped under these circumstances, the evaluator shall ensure the firewall 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.

6 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.

6.1 Security Problem Definition

6.1.1 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 NDPP and include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

6-1 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.

6.1.2 Threats

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

6-2 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.

6.1.3 Organizational Security Policies

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

6.1.4 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.

6-3 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

6.2 Security Objectives

6.2.1 Security Objectives for the TOE

The following table contains security objectives specific to VPN Gateways. These security objectives are in addition to those defined in the NDPP, all of which apply to VPN Gateways. Note that while two of the NDPP security objectives (O.SYSTEM_MONITORING and O.TOE_ADMINISTRATION) have been extended in this EP that does not affect the corresponding security objective definitions.

6-4 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.

6.2.2 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 NDPP, all of which apply to the operational environments for VPN Gateways.

6-5 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.

6.2.3 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.

7 Appendix C: Additional Requirements

7.1.1 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.1.12 element in the body of this EP.

7.1.2 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

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

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

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

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

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

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.

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.

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.

8 Appendix D: Requirements for Mobility

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 NDPP), as well as those specified in this Appendix.

8.1 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.

8.2 Threats

8.2.1 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)

8.2.2 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)

8.2.3 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.

8.3 Objectives

8.3.1 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)

8.3.2 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)

8.3.3 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)

8.4 FTA: TOE Access

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

8.4.1 FTA_SSL.3 TSF-initiated Termination

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

Application Note: This requirement exists in the NDPP, 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 NDPP.

8.4.2 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, [assignment: other attributes]].

Application Note: For this EP, location is defined as the clients IP address.

8.4.3 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.

9 Appendix E

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.

9-1 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

Protocol	Defined Attributes
	Transport Layer Protocol 54 - NBMA Next Hop Resolution Protocol Transport Layer Protocol 61 - any host internal protocol Transport Layer Protocol 62 - CFTP Transport Layer Protocol 63 - any local network Transport Layer Protocol 64 - SATNET and Backroom EXPAK Transport Layer Protocol 65 - Kryptolan Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol Transport Layer Protocol 67 - Internet Pluribus Packet Core Transport Layer Protocol 68 - any distributed file system Transport Layer Protocol 69 - SATNET Monitoring Transport Layer Protocol 70 - VISA Protocol Transport Layer Protocol 71 - Internet Packet Core Utility Transport Layer Protocol 72 - Computer Protocol Network Executive Transport Layer Protocol 73 - Computer Protocol Heart Beat Transport Layer Protocol 74 - Wang Span Network Transport Layer Protocol 75 - Packet Video Protocol Transport Layer Protocol 76 - Backroom SATNET Monitoring Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary Transport Layer Protocol 78 - WIDEBAND Monitoring Transport Layer Protocol 79 - WIDEBAND EXPAK Transport Layer Protocol 80 - ISO Internet Protocol Transport Layer Protocol 81 - VMTP Transport Layer Protocol 82 - SECURE-VMTP Transport Layer Protocol 83 - VINES Transport Layer Protocol 84 - TTP Transport Layer Protocol 85 - NSFNET-IGP Transport Layer Protocol 86 - Dissimilar Gateway Protocol Transport Layer Protocol 87 - TCF Transport Layer Protocol 88 - IGRP Transport Layer Protocol 89 - OSPFIGP Transport Layer Protocol 90 - Sprite RPC Protocol Transport Layer Protocol 91 - Locus Address Resolution Protocol Transport Layer Protocol 92 - Multicast Transport Protocol Transport Layer Protocol 93 - AX.25 Frames Transport Layer Protocol 94 - IP-within-IP Encapsulation Protocol Transport Layer Protocol 95 - Mobile Internetworking Control Protocol Transport Layer Protocol 96 - Semaphore Communications Security Protocol Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation Transport Layer Protocol 98 - Encapsulation Header Transport Layer Protocol 99 - any private encryption scheme Transport Layer Protocol 100 - GMTP
IPv6	Transport Layer Protocol 0 - IPv6 Hop-by-Hop Option 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

Protocol	Defined Attributes
	Transport Layer Protocol 23 - Trunk-1 Transport Layer Protocol 24 - Trunk-2 Transport Layer Protocol 25 - Leaf-1 Transport Layer Protocol 26 - Leaf-2 Transport Layer Protocol 27 - Reliable Data Protocol Transport Layer Protocol 28 - Internet Reliable Transaction Transport Layer Protocol 29 - Transport Protocol Class 4 Transport Layer Protocol 30 - Bulk Data Transfer Protocol Transport Layer Protocol 31 - MFE Network Services Protocol Transport Layer Protocol 32 - MERIT Internodal Protocol Transport Layer Protocol 33 - Datagram Congestion Control Protocol Transport Layer Protocol 34 - Third Party Connect Protocol Transport Layer Protocol 35 - Inter-Domain Policy Routing Protocol Transport Layer Protocol 36 - XTP Transport Layer Protocol 37 - Datagram Delivery Protocol Transport Layer Protocol 38 - IDPR Control Message Transport Proto 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 – Routing Header for IPv6 Transport Layer Protocol 44 – Fragment Header for IPv6 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 - Encap Security Payload Transport Layer Protocol 51 - Authentication Header 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 – Destination Options for IPv6 Transport Layer Protocol 61 - any host internal protocol Transport Layer Protocol 62 - CFTP Transport Layer Protocol 63 - any local network Transport Layer Protocol 64 - SATNET and Backroom EXPAK Transport Layer Protocol 65 - Kryptolan Transport Layer Protocol 66 - MIT Remote Virtual Disk Protocol Transport Layer Protocol 67 - Internet Pluribus Packet Core Transport Layer Protocol 68 - any distributed file system Transport Layer Protocol 69 - SATNET Monitoring Transport Layer Protocol 70 - VISA Protocol Transport Layer Protocol 71 - Internet Packet Core Utility Transport Layer Protocol 72 - Computer Protocol Network Executive Transport Layer Protocol 73 - Computer Protocol Heart Beat Transport Layer Protocol 74 - Wang Span Network Transport Layer Protocol 75 - Packet Video Protocol Transport Layer Protocol 76 - Backroom SATNET Monitoring Transport Layer Protocol 77 - SUN ND PROTOCOL-Temporary Transport Layer Protocol 78 - WIDEBAND Monitoring Transport Layer Protocol 79 - WIDEBAND EXPAK Transport Layer Protocol 80 - ISO Internet Protocol Transport Layer Protocol 81 - VMTP Transport Layer Protocol 82 - SECURE-VMTP Transport Layer Protocol 83 - VINES Transport Layer Protocol 84 - TTP Transport Layer Protocol 84 - Internet Protocol Traffic Manager Transport Layer Protocol 85 - NSFNET-IGP

Protocol	Defined Attributes
	Transport Layer Protocol 86 - Dissimilar Gateway Protocol Transport Layer Protocol 87 - TCF Transport Layer Protocol 88 - EIGRP 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 Pro. Transport Layer Protocol 96 - Semaphore Communications Sec. Pro. Transport Layer Protocol 97 - Ethernet-within-IP Encapsulation Transport Layer Protocol 98 - 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 106 - QNX Transport Layer Protocol 107 - Active Networks Transport Layer Protocol 108 - Payload Compression Protocol Transport Layer Protocol 109 - Sitara Networks Protocol Transport Layer Protocol 110 - Compaq Peer Protocol Transport Layer Protocol 111 - IPX in IP Transport Layer Protocol 112 - Virtual Router Redundancy Protocol Transport Layer Protocol 113 - PGM Reliable Transport Protocol Transport Layer Protocol 114 - any 0-hop protocol Transport Layer Protocol 115 - Layer Two Tunneling Protocol Transport Layer Protocol 116 - D-II Data Exchange (DDX) Transport Layer Protocol 117 - Interactive Agent Transfer Protocol Transport Layer Protocol 118 - Schedule Transfer Protocol Transport Layer Protocol 119 - SpectraLink Radio Protocol Transport Layer Protocol 120 - UTI Transport Layer Protocol 121 - Simple Message Protocol Transport Layer Protocol 122 - SM Transport Layer Protocol 123 - Performance Transparency Protocol Transport Layer Protocol 124 - ISIS over IPv4 Transport Layer Protocol 125 - FIRE Transport Layer Protocol 126 - Combat Radio Transport Protocol Transport Layer Protocol 127 - Combat Radio User Datagram Transport Layer Protocol 128 - SSCOPMCE Transport Layer Protocol 129 - IPLT Transport Layer Protocol 130 - Secure Packet Shield Transport Layer Protocol 131 - Private IP Encapsulation within IP Transport Layer Protocol 132 - Stream Control Transmission Protocol Transport Layer Protocol 133 - Fibre Channel Transport Layer Protocol 134 - RSVP-E2E-IGNORE Transport Layer Protocol 135 - Mobility Header Transport Layer Protocol 136 - UDPLite Transport Layer Protocol 137 - MPLS-in-IP Transport Layer Protocol 138 - MANET Protocols Transport Layer Protocol 139 - Host Identity Protocol Transport Layer Protocol 140 - Shim6 Protocol Transport Layer Protocol 141 - Wrapped Encapsulating Security Payload Transport Layer Protocol 142 - Robust Header Compression