Internet Protocol Security (IPsec) Minimum Essential Interoperability Requirements

Version 1.0.1 FINAL
Core

16 DEC 2011

Prepared By:
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

Table of Contents

List of Tables

1 Internet Protocol Security (IPsec) Minimum Essential Interoperability Requirements

1.1 Networking

Threshold : IPMEIR.NET.1
IPMEIR devices shall support UDP as specified in RFC 768.

1.1.1 Internet Protocol Version 4

Objective : IPMEIR.NET.IPV4.1
IPMEIR devices shall support IPv4 as specified in RFC 791-792.

1.1.2 Internet Protocol Version 6

Threshold : IPMEIR.NET.IPV6.1
IPMEIR devices shall support IPv6 as specified in RFCs 2460-2463.

1.2 Traffic Protection

1.2.1 Cryptography

1.2.1.1 Key Fill

1.2.1.1.1 Internet Key Exchange Version 2

Threshold : IPMEIR.TP.CRYPT.KFILL.IKEV2.1
IPMEIR devices shall treat the first hex character of a Shared Secret HMI entry as the MS Nibble of the MS Byte.

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.3
IPMEIR devices shall allow configuration of a 96 hexadecimal character string through the HMI representing a 384 bit Shared Secret.

Threshold : IPMEIR.TP.CRYPT.KFILL.IKEV2.4
IPMEIR devices shall allow configuration of a 64 hexadecimal character string through the HMI representing a 256 bit Shared Secret.

1.2.1.1.1.1 Certificate

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.1
IPMEIR devices shall support loading of Suite B X.509v3 End Entity Signature Certificates as defined in RFC 5759.

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.2
IPMEIR devices shall support loading of Suite B X.509v3 Self-Signed CA Certificates as defined in RFC 5759.

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.3
IPMEIR devices shall support loading of Suite B X.509v3 Non-Self-Signed CA Certificates as defined in RFC 5759.

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.4
IPMEIR devices shall support loading of Suite B X.509v2 CRLs as defined in RFC 5759.

Objective : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.5
IPMEIR devices shall support Suite B X.509v3 End Entity Signature Certificate Creation with Suite B X.509v3 End Entity Signature Certificates as defined in RFC 5759.

Threshold : IPMEIR.TP.CRYPT.KFILL.IKEV2.CERT.6
If Suite B X.509v3 End Entity Signature Certificate Creation is locally supported, IPMEIR devices shall support Suite B X.509v3 End Entity Signature Certificate exporting with Suite B X.509v3 End Entity Signature Certificates as defined in RFC 5759.

1.2.1.2 Suite B GCM

1.2.1.2.1 Encapsulating Security Payload Version 3

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.1
IPMEIR devices that were the IKE_SA initiator shall populate the 96 bit IV input to GCM with salti concatenated with ESPv3_IV, during encryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.2
IPMEIR devices that were the IKE_SA responder shall populate the 96 bit IV input to GCM with salti concatenated with ESPv3_IV, during decryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.3
IPMEIR devices that were the IKE_SA responder shall populate the 96 bit IV input to GCM with saltr concatenated with ESPv3_IV, during encryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.4
IPMEIR devices that were the IKE_SA initiator shall populate the 96 bit IV input to GCM with saltr concatenated with ESPv3_IV, during decryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.5
IPMEIR devices shall populate the integrity data field of the ESPv3 packet with the 128 bit ICV output of GCM.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.6
IPMEIR devices shall include the SPI concatenated with the Sequence number in the Additional Authenticated Data (AAD) field input to GCM as per Section 5 of RFC 4106 during encryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.7
IPMEIR devices shall include the SPI concatenated with the Sequence number in the Additional Authenticated Data (AAD) field input to GCM as per Section 5 of RFC 4106 during decryption.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.8
IPMEIR devices shall discard all encrypted ESPv3 packets that fail integrity checks of the ICV.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.9
IPMEIR devices shall pad the ESPv3 payload with 0-3 bytes of cryptographic padding such that the size of the encrypted data is aligned on a 4 byte boundary.

Threshold : IPMEIR.TP.CRYPT.SBGCM.ESPV3.10
IPMEIR devices shall populate the ESPv3 Initialization Vector field per RFC 4106 - Section 3.1.

1.2.1.2.2 Internet Key Exchange Version 2

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.1
IPMEIR devices shall discard all IKEv2 packets that fail integrity checks of the Integrity Checksum Data in the IKEv2 encrypted payload.

1.2.1.2.2.1 IKE_SA AES-CBC

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.1
After a successful IKE_SA_INIT exchange, IPMEIR devices shall generate sk_d, sk_ai, sk_ar, sk_ei, sk_er, sk_pi and sk_pr as detailed in Sections 2.13 and 2.14 of RFC 4306.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.2
After a successful IKE_AUTH exchange, IPMEIR devices shall generate sk_ei, salti, sk_er and saltr for the CHILD_SA as detailed in Section 2.17 of RFC 4306 and Section 8.1 of RFC 4106.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.3
After a successful CREATE_CHILD_SA exchange to create a new CHILD_SA, IPMEIR devices shall generate sk_ei, salti, sk_er and saltr for the CHILD_SA as detailed in Section 2.17 of RFC 4306 and Section 8.1 of RFC 4106.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.4
After a successful CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall generate sk_d, sk_ai, sk_ar, sk_ei and sk_er as detailed in Sections 2.13 and 2.14 of RFC 4306.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.5
After a successful CREATE_CHILD_SA exchange to rekey a CHILD_SA, IPMEIR devices shall generate sk_ei, salti, sk_er and saltr for the rekeyed CHILD_SA as detailed in Section 2.17 of RFC 4306 and Section 8.1 of RFC 4106.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.11
IPMEIR devices shall pad the IKEv2 Encrypted Payload with 0-15 bytes of cryptographic padding such that the size of the encrypted data is aligned on a 16 byte boundary.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.12
IPMEIR devices shall populate the Encrypted Payload - Initialization Vector field per RFC 3602 - Section 3.

1.2.1.2.2.1. 128-bit Key-based Suite

Objective : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.1
IPMEIR devices shall support the Suite-B-GCM-128 Suite per RFC 4869.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.2
IPMEIR devices shall support the IKE_SA_INIT exchange with the Suite-B-GCM-128 Suite for the purpose of creating an IKE_SA - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.2.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.2

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENCR_AES_CBC (12)	Key Length (14) - 128
Pseudo-random Function (2)	PRF_HMAC-SHA2_256 (5)	None
Integrity Algorithm (3)	AUTH_HMAC_SHA2_256_128 (12)	None
Diffie-Hellman Group (4)	256-bit random ECP group (19)	None
Per Section 3.1 of RFC 4869.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.3
IPMEIR devices shall support the IKE_AUTH exchange with the Suite-B-GCM-128 Suite for the purpose of creating the first CHILD_SA - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.3.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.3

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 128
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.1 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. Note that the Integrity Algorithm and Diffie-Hellman Group transform types are omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.4
If supporting the CREATE_CHILD_SA exchange to create a new CHILD_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-128 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.4.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.4

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 128
Diffie-Hellman Group (4)	256-bit random ECP group (19)	None
	NONE (0)	None
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.1 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. The Diffie-Hellman Group transform type is ommited if Perfect Forward Secrecy is not desired. Note that the Integrity Algorithm transform type is omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.5
If supporting the CREATE_CHILD_SA exchange for the purpose of re-keying an existing IKE_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-128 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.5.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.5

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENCR_AES_CBC (12)	Key Length (14) - 128
Pseudo-random Function (2)	PRF_HMAC-SHA2_256 (5)	None
Integrity Algorithm (3)	AUTH_HMAC_SHA2_256_128 (12)	None
Diffie-Hellman Group (4)	256-bit random ECP group (19)	None
Per Section 3.1 of RFC 4869.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.6
If supporting the CREATE_CHILD_SA exchange for the purpose of re-keying an existing CHILD_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-128 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.6.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.6

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 128
Diffie-Hellman Group (4)	256-bit random ECP group (19)	None
	NONE (0)	None
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.1 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. The Diffie-Hellman Group transform type is ommited if Perfect Forward Secrecy is not desired. Note that the Integrity Algorithm transform type is omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.7
IPMEIR devices shall populate the Key Exchange Data of the Key Exchange Payload with the Diffie-Hellman public key of total length 512 bits per Section 8.1 of RFC 5903 when negotiating a 256-bit random ECP group.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.8
When using 256-bit random ECP group (19), IPMEIR devices shall derive the Diffie-Hellman Shared Secret (girx) per Section 8.1 of RFC 5903.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S128.9
IPMEIR devices shall populate the 128 bit Integrity Checksum Data field of the IKEv2 encrypted payload with the 128 bit ICV output of HMAC-SHA256-128.

1.2.1.2.2.1. 256-bit Key-based Suite

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.1
IPMEIR devices shall support the Suite-B-GCM-256 Suite per RFC 4869.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.2
IPMEIR devices shall support the IKE_SA_INIT exchange with the Suite-B-GCM-256 Suite for the purpose of creating an IKE_SA - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.2.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.2

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENCR_AES_CBC (12)	Key Length (14) - 256
Pseudo-random Function (2)	PRF_HMAC-SHA2_384 (6)	None
Integrity Algorithm (3)	AUTH_HMAC_SHA2_384_192 (13)	None
Diffie-Hellman Group (4)	384-bit random ECP group (20)	None
Per Section 3.2 of RFC 4869.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.3
IPMEIR devices shall support the IKE_AUTH exchange with the Suite-B-GCM-256 Suite for the purpose of creating the first CHILD_SA - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.3.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.3

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 256
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.2 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. Note that the Integrity Algorithm and Diffie-Hellman Group transform types are omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.4
If supporting the CREATE_CHILD_SA exchange to create a new CHILD_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-256 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.4.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.4

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 256
Diffie-Hellman Group (4)	384-bit random ECP group (20)	None
	NONE (0)	None
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.2 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. The Diffie-Hellman Group transform type is ommited if Perfect Forward Secrecy is not desired. Note that the Integrity Algorithm transform type is omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.5
If supporting the CREATE_CHILD_SA exchange for the purpose of re-keying an existing IKE_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-256 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.5.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.5

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENCR_AES_CBC (12)	Key Length (14) - 256
Pseudo-random Function (2)	PRF_HMAC-SHA2_384 (6)	None
Integrity Algorithm (3)	AUTH_HMAC_SHA2_384_192 (13)	None
Diffie-Hellman Group (4)	384-bit random ECP group (20)	None
Per Section 3.2 of RFC 4869.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.6
If supporting the CREATE_CHILD_SA exchange for the purpose of re-keying an existing CHILD_SA, IPMEIR devices shall support the CREATE_CHILD_SA exchange with the Suite-B-GCM-256 Suite - the Transform types and their associated transform IDs and Attributes are shown in Table IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.6.

Table - IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.6

Transform Type	Transform ID	Transform Attribute - Value
Encryption Algorithm (1)	ENC_AES_GCM (20)	Key Length (14) - 256
Diffie-Hellman Group (4)	384-bit random ECP group (20)	None
	NONE (0)	None
Extended Sequence Numbers (5)	No Extended Sequence Numbers (0)	None
	Extended Sequence Numbers (1)	None
Per Section 3.2 of RFC 4869. Per IPMEIR.TP.IKEV2.83, Extended Sequence Numbers are objective. The Diffie-Hellman Group transform type is ommited if Perfect Forward Secrecy is not desired. Note that the Integrity Algorithm transform type is omitted from the SA Payload.		

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.7
IPMEIR devices shall populate the Key Exchange Data of the Key Exchange Payload with the Diffie-Hellman public key of total length 768 bits per Section 8.2 of RFC 5903 when negotiating a 384-bit random ECP group.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.8
When using 384-bit random ECP group (20), IPMEIR devices shall derive the Diffie-Hellman Shared Secret (girx) per Section 8.2 of RFC 5903.

Threshold : IPMEIR.TP.CRYPT.SBGCM.IKEV2.ISACBC.S256.9
IPMEIR devices shall populate the 192 bit Integrity Checksum Data field of the IKEv2 encrypted payload with the 192 bit ICV output of HMAC-SHA384-192.

1.2.2 Encapsulating Security Payload Version 3

Threshold : IPMEIR.TP.ESPV3.1
IPMEIR devices shall initialize the Sliding Window Counter to ZERO, dropping any received packet with a Sequence Number of ZERO on an SA.

Threshold : IPMEIR.TP.ESPV3.2
IPMEIR devices shall verify that a received packet contains a sequence number that is not a duplicate for the life of the SA.

Threshold : IPMEIR.TP.ESPV3.3
IPMEIR devices shall reset the Sequence Number to ZERO such that when the SPI of an SA changes due to a rekey the first packet transmitted under the new SA contains a Sequence Number of one.

Threshold : IPMEIR.TP.ESPV3.4
IPMEIR devices shall increment the Sequence Number for every transmitted packet.

Threshold : IPMEIR.TP.ESPV3.5
IPMEIR devices shall discard all packets received with the Value 59 Decimal specified in the Next Header field of the ESP trailer without indicating an error.

Threshold : IPMEIR.TP.ESPV3.6
When supporting a 32 bit sequence number, IPMEIR devices shall rekey or delete an SA prior to the transmission of the 2^32nd packet on that SA.

Threshold : IPMEIR.TP.ESPV3.7
When supporting a 64 bit sequence number, IPMEIR devices shall rekey or delete an SA prior to the transmission of the 2^64th packet on that SA.

1.2.2.1 Network Address Translation Traversal

Threshold : IPMEIR.TP.ESPV3.NAT-T.1
When a NAT device has been detected, IPMEIR devices shall encapsulate all subsequent ESP traffic on the SA in UDP datagrams.

Threshold : IPMEIR.TP.ESPV3.NAT-T.2
When encapsulating ESP in UDP, IPMEIR devices shall format the UDP header as detailed in Table - IPMEIR.TP.ESPV3.NAT-T.2.

Table - IPMEIR.TP.ESPV3.NAT-T.2

Field	Size	Value
Source Port	16-bits	4500 decimal
Destination Port	16-bits	Initiator=4500 decimal
		Responder=Variable
Length	16-bits	The length in octets of this datagram including this header and the data.
Checksum	16-bits	Set to ZERO (0).

Threshold : IPMEIR.TP.ESPV3.NAT-T.3
IPMEIR devices shall not validate the UDP Checksum of packets received on port 4500.

Threshold : IPMEIR.TP.ESPV3.NAT-T.4
When a NAT device has been detected, the initiating IPMEIR device shall set the encapsulating UDP Source and Destination ports of all ESP traffic to 4500.

Threshold : IPMEIR.TP.ESPV3.NAT-T.5
When NAT traversal is in use, responding IPMEIR devices shall use the source address and source port received in messages as the destination address and destination port for the IP-UDP header of packets transmitted on the associated SA.

1.2.2.1.1 Tunnel Mode

Threshold : IPMEIR.TP.ESPV3.NAT-T.TNMD.1
When Tunnel Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Tunnel Mode Decapsulation NAT Procedure detailed in RFC 3948, Section 3.1.1 #1.

Threshold : IPMEIR.TP.ESPV3.NAT-T.TNMD.2
When Tunnel Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Tunnel Mode ESP Encapsulation procedure detailed in RFC 3948, Section 3.4.

Threshold : IPMEIR.TP.ESPV3.NAT-T.TNMD.3
When Tunnel Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Tunnel Mode ESP Decapsulation procedure detailed in RFC 3948, Section 3.5.

1.2.2.1.2 Transport Mode

Threshold : IPMEIR.TP.ESPV3.NAT-T.TRPMD.1
When Transport Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Transport Mode Decapsulation NAT Procedure detailed in RFC 3948, Section 3.1.2 #1.

Threshold : IPMEIR.TP.ESPV3.NAT-T.TRPMD.2
When Transport Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Transport Mode ESP Encapsulation procedure detailed in RFC 3948, Section 3.2.

Threshold : IPMEIR.TP.ESPV3.NAT-T.TRPMD.3
When Transport Mode has been negotiated, IPMEIR devices performing NAT Traversal shall use the Transport Mode ESP Decapsulation procedure detailed in RFC 3948, Section 3.3.

1.2.2.2 Tunnel Mode

Threshold : IPMEIR.TP.ESPV3.TNMD.1
IPMEIR devices shall support reception and transmission of user data in ESPv3 Tunnel Mode.

Threshold : IPMEIR.TP.ESPV3.TNMD.2
IPMEIR devices shall format ESPv3 Tunnel Mode packet as specified in Table - IPMEIR.TP.ESPV3.TNMD.2.

Table - IPMEIR.TP.ESPV3.TNMD.2

Field	Size
CT IP Header	Variable
Security Parameter Index (SPI)	32 bits
Sequence Number	32 bits
Initialization Vector (IV)	Variable
Original IP Packet	Variable
Cryptographic Padding	Variable (0-255 octets)
Pad Length	8 bits
Next Header	8 bits
Integrity Check Value	Variable

Threshold : IPMEIR.TP.ESPV3.TNMD.3
IPMEIR devices shall encrypt all information from the Original IP Packet to the Next Header fields inclusive.

Threshold : IPMEIR.TP.ESPV3.TNMD.4
IPMEIR devices shall be able to decrypt and properly decapsulate an inner IP packet concatenated with TFC pad octets.

1.2.2.3 Transport Mode

Objective : IPMEIR.TP.ESPV3.TRPMD.1
IPMEIR devices shall support reception and transmission of user data in ESPv3 Transport Mode.

Threshold : IPMEIR.TP.ESPV3.TRPMD.2
IPMEIR devices shall format ESPv3 Transport Mode packets as specified in Table - IPMEIR.TP.ESPV3.TRPMD.2.

Table - IPMEIR.TP.ESPV3.TRPMD.2

Field	Size
CT IP Header	Variable
Security Parameter Index (SPI)	32 bits
Sequence Number	32 bits
Initialization Vector (IV)	Variable
Transport Layer Datagram	Variable
Cryptographic Padding	Variable (0-255 octets)
Pad Length	8 bits
Next Header	8 bits
Integrity Check Value	Variable

Threshold : IPMEIR.TP.ESPV3.TRPMD.3
IPMEIR devices shall encrypt all information from the Transport Layer Datagram to the Next Header fields inclusive.

Threshold : IPMEIR.TP.ESPV3.TRPMD.4
During encapsulation of an ESPv3 Transport Mode packet, IPMEIR devices shall copy the PT IP header's Next Header (IPv6) or Protocol (IPv4) field as appropriate, into the ESPv3 Trailer Next Header field.

1.2.3 Internet Key Exchange Version 2

Threshold : IPMEIR.TP.IKEV2.1
When sending an IKE_SA_INIT request message, IPMEIR devices shall send the request message addressed to UDP Destination port 500.

Threshold : IPMEIR.TP.IKEV2.2
IPMEIR devices shall accept IKE messages from any UDP Source port.

Threshold : IPMEIR.TP.IKEV2.3
IPMEIR devices shall send all IKE messages addressed to the IP Address and UDP Destination port from which it receives IKE messages.

Threshold : IPMEIR.TP.IKEV2.4
IPMEIR devices shall be able to accept and process an IKE request message while it has an IKE request message outstanding.

Threshold : IPMEIR.TP.IKEV2.5
IPMEIR devices shall delete the IKE_SA or initiate a CREATE_CHILD_SA exchange to rekey the IKE_SA prior to the Message ID reaching (2^32)-1.

Threshold : IPMEIR.TP.IKEV2.6
After a successful IKE_SA_INIT exchange, upon receipt of a retransmitted IKE request message within the declared Window Size, IPMEIR devices shall retransmit the corresponding IKE response message.

Threshold : IPMEIR.TP.IKEV2.7
IPMEIR devices shall not send payloads with the Critical Bit set to ONE unless specified herein.

Threshold : IPMEIR.TP.IKEV2.8

IPMEIR devices shall format the IKE_SA_INIT request message as shown in Table - IPMEIR.TP.IKEV2.8.

Table - IPMEIR.TP.IKEV2.8

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	0 decimal
	Next Payload (8-bits)	33 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	34 decimal
	Flags (8-bits)	00001000 (binary)
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	0 decimal
	Length (32-bits)	Per RFC 4306 Section 3.1.
Security Association Payload	Next Payload (8-bits)	34 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Per RFC 4306 Section 3.3.1.
	Protocol ID (8-bits)	1 decimal
	SPI Size (8-bits)	0 decimal
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Per RFC 4306 Section 3.3.2.
	Attribute Type (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Length (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Value (variable)	Per RFC 4306 Section 3.3.5.
Key Exchange Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Diffie-Hellman Group Number (16-bits)	Per RFC 4306 Section 3.4.
	RESERVED (16-bits)	0 decimal
	Key Exchange Data (variable)	Per RFC 4306 Section 3.4
Nonce Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9.

Threshold : IPMEIR.TP.IKEV2.9

IPMEIR devices shall format the IKE_SA_INIT response message as shown in Table - IPMEIR.TP.IKEV2.9.

Table - IPMEIR.TP.IKEV2.9

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	33 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	34 decimal
	Flags (8-bits)	00100000 (binary)
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	0 decimal
	Length (32-bits)	Per RFC 4306 Section 3.1.
Security Association Payload	Next Payload (8-bits)	34 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Proposal Number corresponding to selected proposal.
	Protocol ID (8-bits)	1 decimal
	SPI Size (8-bits)	0 decimal
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Transform ID corresponding to selected transform.
	Attribute Type (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Length (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Value (variable)	Data Attributes corresponding to selected transform.
Key Exchange Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Diffie-Hellman Group Number (16-bits)	Diffie-Hellman Group Number corresponding to selected Diffie-Hellman group.
	RESERVED (16-bits)	0 decimal
	Key Exchange Data (variable)	Per RFC 4306 Section 3.4 and negotiated IPMEIR cryptographic suite.

Nonce Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9 and negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.10
When sending an IKE_SA_INIT message, IPMEIR devices shall generate nonces such that the length is at least half the key size of the largest proposed pseudo-random function in the Security Association Payload.

Threshold : IPMEIR.TP.IKEV2.11
After a successful IKE_SA_INIT exchange, IPMEIR devices shall generate SKEYSEED as detailed in RFC 4306 Section 2.14.

Threshold : IPMEIR.TP.IKEV2.12
After a successful IKE_SA_INIT exchange, IPMEIR devices shall set the Window Size to ONE.

Threshold : IPMEIR.TP.IKEV2.13
IPMEIR devices shall not use SPI values 0-255, when negotiating an ESPv3 CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.14
IPMEIR devices shall format the IKE_AUTH request message as shown in Table - IPMEIR.TP.IKEV2.14.

Table - IPMEIR.TP.IKEV2.14

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	35 decimal
	Flags (8-bits)	00001000 (binary)
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	1 decimal
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	35 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Identification - Initiator Payload	Next Payload (8-bits)	39 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	ID Type (8-bits)	5 decimal (ID_IPV6_ADDR when operating in IPv6). See IPMEIR.TP.IKEV2.15.
		1 decimal (ID_IPV4_ADDR when operating in IPv4). See IPMEIR.TP.IKEV2.90.
	RESERVED (24-bits)	0 decimal
	Identification Data (Variable)	A single 16-octet IPv6 address.
		A single 4-octet IPv4 address.

Authentication Payload	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Auth Method (8-bits)	2 decimal (for Shared Key Message Integrity Code)
		9 decimal (for ECDSA with SHA-256 on the P-256 curve)
		10 decimal (for ECDSA with SHA-384 on the P-384 curve)
	RESERVED (24-bits)	0 decimal
	Authentication Data (variable)	See IPMEIR.TP.IKEV2.17 for Shared Key Message Integrity Code.
		See IPMEIR.TP.IKEV2.CERT.15 for ECDSA with SHA-256 on the P-256 curve.
		See IPMEIR.TP.IKEV2.CERT.17 for ECDSA with SHA-384 on the P-384 curve.
Security Association Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Per RFC 4306 Section 3.3.1.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Per RFC 4306 Section 3.3.2.
	Attribute Type (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Length (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Value (variable)	Per RFC 4306 Section 3.3.5.
Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.

	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.15
When operating in IPv6, IPMEIR devices shall support sending an Identification - Initiator/Responder Payload with an Identification Type of ID_IPV6_ADDR.

Threshold : IPMEIR.TP.IKEV2.16
When operating in IPv6, IPMEIR devices shall support receipt of an Identification - Initiator/Responder Payload containing Identification Types ID_IPV6_ADDR, ID_FQDN, ID_RFC822_ADDR, or ID_KEY_ID.

Threshold : IPMEIR.TP.IKEV2.17
When using Authentication Method-Shared Key Message Integrity Code in the IKE_AUTH request Authentication Payload, IPMEIR devices shall populate the Authentication Data prf(prf(Shared Secret, "Key Pad for IKEv2"), msg octets). Note: "Key Pad for IKEv2" is defined as the binary representation of the string "Key Pad for IKEv2" not including quotation marks; msg octets (see Authentication Payload) is the InitiatorSignedOctets and is defined as the following: InitiatorSignedOctets = RealMessage1 | NonceRData | MACedIDForI; GenIKEHDR = [four octets 0 if using port 4500] | RealIKEHDR; RealIKEHDR = SPIi | SPIr | . . . | Length; RealMessage1 = RealIKEHDR | RestOfMessage1; NonceRPayload = PayloadHeader | NonceRData; InitiatorIDPayload = PayloadHeader | RestOfInitIDPayloa; RestOfInitIDPayload = IDType | RESERVED | InitIDData; MACedIDForI = prf(sk_pi, RestOfInitIDPayload).

Threshold : IPMEIR.TP.IKEV2.18
IPMEIR devices shall format the IKE_AUTH response message as shown in Table - IPMEIR.TP.IKEV2.18.

Table - IPMEIR.TP.IKEV2.18

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	35 decimal
	Flags (8-bits)	00100000 (binary)
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	1 decimal
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	36 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Identification - Responder Payload	Next Payload (8-bits)	39 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	ID Type (8-bits)	5 decimal (ID_IPV6_ADDR when operating in IPv6). See IPMEIR.TP.IKEV2.15.
		1 decimal (ID_IPV4_ADDR when operating in IPv4). See IPMEIR.TP.IKEV2.90.
	RESERVED (24-bits)	0 decimal
	Identification Data (Variable)	A single 16-octet IPv6 address.
		A single 4-octet IPv4 address.

Authentication Payload	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Auth Method (8-bits)	2 decimal (for Shared Key Message Integrity Code)
		9 decimal (for ECDSA with SHA-256 on the P-256 curve)
		10 decimal (for ECDSA with SHA-384 on the P-384 curve)
	RESERVED (24-bits)	0 decimal
	Authentication Data (variable)	See IPMEIR.TP.IKEV2.19 for Shared Key Message Integrity Code.
		See IPMEIR.TP.IKEV2.CERT.16 for ECDSA with SHA-256 on the P-256 curve.
		See IPMEIR.TP.IKEV2.CERT.18 for ECDSA with SHA-384 on the P-384 curve.
Security Association Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Proposal Number corresponding to selected proposal.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Transform ID corresponding to selected transform.
	Attribute Type (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Length (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Value (variable)	Data Attributes corresponding to selected transform.
Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.

	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.19
When using Authentication Method-Shared Key Message Integrity Code in the IKE_AUTH response Authentication Payload, IPMEIR devices shall populate the Authentication Data with prf(prf(Shared Secret, "Key Pad for IKEv2"), msg octets). Note: "Key Pad for IKEv2" is defined as the binary representation of the string "Key Pad for IKEv2" not including quotation marks; msg octets (see Authentication Payload) is the ResponderSignedOctets and is defined as the following: ResponderSignedOctets = RealMessage2 | NonceIData | MACedIDForR; GenIKEHDR = [four octets 0 if using port 4500] | RealIKEHDR; RealIKEHDR = SPIi | SPIr | . . . | Length; RealMessage2 = RealIKEHDR | RestOfMessage2; NonceIPayload = PayloadHeader | NonceIData; ResponderIDPayload = PayloadHeader | RestOfRespIDPayload; RestOfRespIDPayload = IDType | RESERVED | RespIDData; MACedIDForR = prf(sk_pr, RestOfRespIDPayload).

Threshold : IPMEIR.TP.IKEV2.20
IPMEIR devices shall validate the Authentication Data and terminate the IKE exchange if the validation fails.

Threshold : IPMEIR.TP.IKEV2.21
When sending the N(NO_ADDITIONAL_SAS) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.21.

Table - IPMEIR.TP.IKEV2.21

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(NO_ADDITIONAL_SAS) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	35 decimal

Threshold : IPMEIR.TP.IKEV2.22

IPMEIR devices shall format the INFORMATIONAL request message as shown in Table - IPMEIR.TP.IKEV2.22.

Table - IPMEIR.TP.IKEV2.22

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	37 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.23
IPMEIR devices shall format the INFORMATIONAL response message as shown in Table - IPMEIR.TP.IKEV2.23.

Table - IPMEIR.TP.IKEV2.23

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	37 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.24
Upon receipt of an Security Association Payload in a request message, IPMEIR devices shall select one Transform ID for each Transform Type proposed in the selected proposal.

Threshold : IPMEIR.TP.IKEV2.27
IPMEIR devices shall ignore unknown Transform Types and be able to continue processing a Security Association Payload.

Threshold : IPMEIR.TP.IKEV2.28
IPMEIR devices shall ignore unknown Transform IDs and be able to continue processing a Security Association Payload.

Threshold : IPMEIR.TP.IKEV2.29
IPMEIR devices shall ignore unknown Attribute Types and be able to continue processing a Security Association Payload.

Threshold : IPMEIR.TP.IKEV2.30
Upon receipt of an IKE_SA_INIT request message, if none of the proposed cryptographic suites are acceptable by policy, IPMEIR devices shall send an IKE_SA_INIT response message with a N(NO_PROPOSAL_CHOSEN) Payload as the only payload within the IKE_SA_INIT response message.

Threshold : IPMEIR.TP.IKEV2.31
Upon receipt of a CHILD_SA request message, if none of the proposed cryptographic suites are acceptable by policy, IPMEIR devices shall send a CHILD_SA response message with a N(NO_PROPOSAL_CHOSEN) Payload; the N(NO_PROPOSAL_CHOSEN) Payload shall be placed within the Encrypted Payload, and the Security Association Payload, Traffic Selector - Initiator Payload, Traffic Selector - Responder Payload, and Key Exchange Payload (if applicable) shall be omitted.

Threshold : IPMEIR.TP.IKEV2.32
When sending the N(NO_PROPOSAL_CHOSEN) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.32.

Table - IPMEIR.TP.IKEV2.32

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(NO_PROPOSAL_CHOSEN) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	14 decimal

Threshold : IPMEIR.TP.IKEV2.33
Upon receipt of an IKE_SA_INIT request message, if a proposed cryptographic suite is acceptable but the Diffie-Hellman value received in the Key Exchange Payload was incorrect, IPMEIR devices shall send an IKE_SA_INIT response message with a N(INVALID_KE_PAYLOAD) Payload as the only payload within the IKE_SA_INIT response message.

Threshold : IPMEIR.TP.IKEV2.34
When sending the N(INVALID_KE_PAYLOAD) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.34.

Table - IPMEIR.TP.IKEV2.34

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(INVALID_KE_PAYLOAD) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	10 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bits	17 decimal
Notification Data	16-bits	Accepted Diffie-Hellman Group. Per RFC 4306 Section 3.10.1.

Threshold : IPMEIR.TP.IKEV2.35
If the CHILD_SA request message was generated by an outgoing plaintext packet, IPMEIR devices shall include the source address, source port and protocol of the outgoing plaintext packet as the first traffic selector in the Traffic Selector - Initiator Payload.

Threshold : IPMEIR.TP.IKEV2.36
If the CHILD_SA request message was generated by an outgoing plaintext packet, IPMEIR devices shall include the destination address, destination port and protocol of the outgoing plaintext packet as the first traffic selector in the Traffic Selector - Responder Payload.

Threshold : IPMEIR.TP.IKEV2.37
Upon receipt of an IKE_AUTH request message where none of the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload are acceptable by policy, IPMEIR devices shall send an IKE_AUTH response message with a N(TS_UNACCEPTABLE) Payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.38
When sending the N(TS_UNACCEPTABLE) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.38.

Table - IPMEIR.TP.IKEV2.38

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(TS_UNACCEPTABLE) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	38 decimal

Threshold : IPMEIR.TP.IKEV2.39
Upon receipt of a CHILD_SA request message where all the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload are acceptable by policy, IPMEIR devices shall send a CHILD_SA response message with a Traffic Selector - Initiator and a Traffic Selector - Responder Payload identical to the one received in the CHILD_SA request message.

Threshold : IPMEIR.TP.IKEV2.40
Upon receipt of a CHILD_SA request message where the union of all subset(s) of the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload is acceptable by policy, IPMEIR devices shall send a CHILD_SA response message with a Traffic Selector - Initiator Payload and Traffic Selector - Responder Payload containing the subset(s) of traffic selectors.

Threshold : IPMEIR.TP.IKEV2.41
Upon receipt of a CHILD_SA request message where the union of subsets of the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload is not acceptable by policy but one of the acceptable subsets contains the specific traffic selector source address and destination address that initiated the CHILD_SA request message, IPMEIR devices shall send a CHILD_SA response message with a Traffic Selector - Initiator Payload and Traffic Selector - Responder Payload containing the subset of traffic selectors that encompasses the specific traffic selector source address and destination address.

Threshold : IPMEIR.TP.IKEV2.42
Upon receipt of a CHILD_SA request message where the union of subsets of the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload is not acceptable by policy, IPMEIR devices shall send a CHILD_SA response message with a Traffic Selector - Initiator Payload and Traffic Selector - Responder Payload containing an arbitrarily chosen acceptable subset of traffic selectors.

Threshold : IPMEIR.TP.IKEV2.43
When sending the N(ADDITIONAL_TS_POSSIBLE) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.43.

Table - IPMEIR.TP.IKEV2.43

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(ADDITIONAL_TS_POSSIBLE) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16386 decimal

Objective : IPMEIR.TP.IKEV2.44
When deleting an IKE_SA, IPMEIR devices shall send an INFORMATIONAL request message with a Delete Payload.

Threshold : IPMEIR.TP.IKEV2.45
Upon receipt of an INFORMATIONAL request message with a Delete Payload to delete an IKE_SA, IPMEIR devices shall send an empty INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.46
When sending the Delete Payload to delete an IKE_SA, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.46.

Table - IPMEIR.TP.IKEV2.46

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2.
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	1 decimal
SPI Size	8-bits	0 decimal
# of SPIs	16-bit	0 decimal

Threshold : IPMEIR.TP.IKEV2.47
When deleting a CHILD_SA(s), IPMEIR devices shall send an INFORMATIONAL request message with a Delete Payload.

Threshold : IPMEIR.TP.IKEV2.48
Upon receipt of an INFORMATIONAL request message with a Delete Payload to delete a CHILD_SA(s), IPMEIR devices shall include a Delete Payload in the INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.49
When sending the Delete Payload to delete a CHILD_SA(s), IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.49.

Table - IPMEIR.TP.IKEV2.49

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the payload (or the IKE Header) preceding the Delete Payload as 0x2A (decimal 42).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	Per RFC 4306 Section 3.2.
Protocol ID	8-bits	3 decimal
SPI Size	8-bits	4 decimal
# of SPIs	16-bit	Per RFC 4306 Section 3.11.
SPI(s)	Variable	Per RFC 4306 Section 3.11; SPI(s) of inbound CHILD_SA(s) to be deleted.

Threshold : IPMEIR.TP.IKEV2.50
IPMEIR devices shall be able to process an INFORMATIONAL request message with multiple Delete Payloads.

Threshold : IPMEIR.TP.IKEV2.53
Upon receipt of a CREATE_CHILD_SA request message to rekey an IKE_SA and the IPMEIR device is in the process of creating, rekeying or deleting a CHILD_SA, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_PROPOSAL_CHOSEN) Payload as the only payload within the Encrypted Payload of the CREATE_CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.56
Upon receipt of an INFORMATIONAL request message with a Delete Payload to delete a CHILD_SA(s) that does not exist or the IPMEIR device is in the process of deleting, IPMEIR devices shall send an INFORMATIONAL response message without a corresponding Delete Payload(s).

Threshold : IPMEIR.TP.IKEV2.59
Upon receipt of an unknown payload with a Critical Bit set to ZERO, IPMEIR devices shall be able to process the Next Payload, Critical Bit, Reserved, and Payload Length fields to determine the beginning of the next payload to process.

Threshold : IPMEIR.TP.IKEV2.60
Upon receipt of an IKE request message with an unfamiliar payload with the Critical Bit set to ONE, IPMEIR devices shall reject the IKE request message and deem that the exchange has failed entirely.

Threshold : IPMEIR.TP.IKEV2.61
When sending the N(UNSUPPORTED_CRITICAL_PAYLOAD) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.61.

Table - IPMEIR.TP.IKEV2.61

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(UNSUPPORTED_CRITICAL_PAYLOAD) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	9 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	1 decimal
Notification Data	8-bits	Payload Type of the unrecognized Critical Payload.

Threshold : IPMEIR.TP.IKEV2.62
Upon receipt of an INFORMATIONAL request message with a N(SET_WINDOW_SIZE) Payload as the only payload in the INFORMATIONAL request message, IPMEIR devices shall send a corresponding empty INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.63
IPMEIR devices shall support the receipt of a N(SET_WINDOW_SIZE) Payload in any IKE message.

Threshold : IPMEIR.TP.IKEV2.64
After the establishment of the IKE_SA, upon receipt of an IKE message with Message ID outside the supported Window Size, IPMEIR devices shall drop the message.

Threshold : IPMEIR.TP.IKEV2.66
Upon receipt of an IKE_SA_INIT response message with a N(COOKIE) Payload, IPMEIR devices shall retransmit the IKE_SA_INIT request message with payloads identical to the payloads sent in the preceding IKE_SA_INIT request message and include the N(COOKIE) Payload, identical to the one received in the IKE_SA_INIT response message, in the retransmitted IKE_SA_INIT request message.

Threshold : IPMEIR.TP.IKEV2.67
Upon receipt of an INFORMATIONAL response message without a corresponding Delete Payload(s) to delete a CHILD_SA(s), IPMEIR devices shall locally delete the CHILD_SA pair(s) as indicated by the SPI(s) in the Delete Payload(s) sent in the corresponding INFORMATIONAL request message.

Threshold : IPMEIR.TP.IKEV2.68
If there are no other IKE_SAs established with the to-be-established authenticated identity, IPMEIR devices shall include a N(INITIAL_CONTACT) Payload in the IKE_AUTH request message within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.69
When sending the N(INITIAL_CONTACT) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.69.

Table - IPMEIR.TP.IKEV2.69

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the payload preceding the N(INITIAL_CONTACT) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16384 decimal

Threshold : IPMEIR.TP.IKEV2.70
Upon receipt of a N(INITIAL_CONTACT) Payload in a successfully validated IKE_AUTH request message, IPMEIR devices shall locally delete any previously existing IKE_SA established with the authenticated identity and any CHILD_SAs parented by the IKE_SAs.

Threshold : IPMEIR.TP.IKEV2.72
When using Authentication Method-Shared Key Message Integrity Code in the IKE_AUTH request Authentication Payload, IPMEIR devices shall use the Shared Secret associated with the Identification Data of the Identification - Initiator Payload for the calculation of the Authentication Data.

Threshold : IPMEIR.TP.IKEV2.73
When using Authentication Method-Shared Key Message Integrity Code in the IKE_AUTH response Authentication Payload, IPMEIR devices shall use the Shared Secret associated with the Identification Data of the Identification - Responder Payload for the calculation of the Authentication Data.

Threshold : IPMEIR.TP.IKEV2.74
Upon receipt of an IKE_AUTH request message, if the Authentication Data does not validate, IPMEIR devices shall send an IKE_AUTH response message with a N(AUTHENTICATION_FAILED) Payload as the only payload within the IKE_AUTH response message.

Threshold : IPMEIR.TP.IKEV2.75
Upon receipt of an IKE_AUTH request message, if the Identification Data of the Identification - Initiator Payload can not be matched and thus a Shared Secret can not be associated, IPMEIR devices shall send an IKE_AUTH response message with a N(AUTHENTICATION_FAILED) Payload as the only payload within the IKE_AUTH response message.

Threshold : IPMEIR.TP.IKEV2.76
When sending the N(AUTHENTICATION_FAILED) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.76.

Table - IPMEIR.TP.IKEV2.76

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(AUTHENTICATION_FAILED) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	24 decimal

Threshold : IPMEIR.TP.IKEV2.77
Upon the receipt of an IKE response message containing a Notify Payload - Notify Message Type with an unknown Error Type, IPMEIR devices shall deem that the corresponding IKE request has failed entirely.

Threshold : IPMEIR.TP.IKEV2.78
Upon the receipt of an IKE request message containing a Notify Payload - Notify Message Type with an unknown Error Type, IPMEIR devices shall ignore the Notify Payload and continue processing.

Threshold : IPMEIR.TP.IKEV2.79
Upon the receipt of an IKE request message containing a Notify Payload - Notify Message Type with an unknown Status Type, IPMEIR devices shall ignore the Notify Payload and continue processing.

Threshold : IPMEIR.TP.IKEV2.80
Upon the receipt of an IKE response message containing a Notify Payload - Notify Message Type with an unknown Status Type, IPMEIR devices shall ignore the Notify Payload and continue processing.

Threshold : IPMEIR.TP.IKEV2.81
Upon the receipt of an unfamiliar Vendor ID Payload - Vendor ID, IPMEIR devices shall be able to process the Next Payload, Critical Bit, Reserved, and Payload Length fields to determine the beginning of the next payload to process.

Threshold : IPMEIR.TP.IKEV2.82
IPMEIR devices shall be able to process IKE messages with payloads organized in any order except where otherwise specified herein or in RFC 4306.

Objective : IPMEIR.TP.IKEV2.83
IPMEIR devices shall support the negotiation of Extended Sequence Numbers for ESPv3 CHILD_SAs.

Threshold : IPMEIR.TP.IKEV2.84
Upon successful completion of an IKE_SA_INIT exchange and the subsequent IKE_AUTH exchange, IPMEIR devices shall use the new sk_ei/sk_er to protect IKE_SA traffic on the newly-created IKE_SA.

Threshold : IPMEIR.TP.IKEV2.85
Upon successful completion of an IKE_AUTH exchange, IPMEIR devices shall use the new sk_ei/sk_er to protect CHILD_SA traffic on the newly-created CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.86
Upon receipt of a Delete Payload to delete an IKE_SA, IPMEIR devices shall release the IKE_SA and the associated CHILD_SAs if the identified IKE Initiator's SPI and IKE Responder's SPI are valid for the source IPMEIR device sending the Delete Payload.

Threshold : IPMEIR.TP.IKEV2.88
Upon receipt of a Delete Payload to delete a CHILD_SA(s), IPMEIR devices shall release the identified CHILD_SA(s) if the identified SPI(s) are valid for the source IPMEIR device sending the Delete Payload.

Threshold : IPMEIR.TP.IKEV2.89
Upon receipt of a CREATE_CHILD_SA request message to rekey an SA, if rekeying is not supported, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_ADDITIONAL_SAS) Payload as the only payload within the Encrypted Payload as shown in Table - IPMEIR.TP.IKEV2.21.

Threshold : IPMEIR.TP.IKEV2.90
When operating in IPv4, IPMEIR devices shall support sending an Identification - Initiator/Responder Payload with an Identification Type of ID_IPV4_ADDR.

Threshold : IPMEIR.TP.IKEV2.91
When operating in IPv4, IPMEIR devices shall support receipt of an Identification - Initiator/Responder Payload containing Identification Types ID_IPV4_ADDR, ID_FQDN, ID_RFC822_ADDR, or ID_KEY_ID.

Threshold : IPMEIR.TP.IKEV2.92
Upon receipt of a CREATE_CHILD_SA request message where none of the traffic selectors proposed in the Traffic Selector - Initiator Payload and the Traffic Selector - Responder Payload are acceptable by policy, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(TS_UNACCEPTABLE) Payload as the only payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.93
Upon receipt of an INFORMATIONAL request message without cryptographic protection IPMEIR devices must not respond with an unprotected INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.94
IPMEIR devices shall ignore the Critical Bit for supported IKE payloads.

Threshold : IPMEIR.TP.IKEV2.95
Upon receipt of a message with a higher major version number, IPMEIR devices shall drop the message and send an unauthenticated N(INVALID_MAJOR_VERSION) notification containing the highest version number it supports.

Threshold : IPMEIR.TP.IKEV2.96
When parsing a Security Association payload, IPMEIR devices must check that the total Payload Length is consistent with the payload's internal lengths and counts.

Threshold : IPMEIR.TP.IKEV2.97
IPMEIR devices shall support the Initiator use of UDP port 4500 regardless of whether or not there is a NAT, even at the beginning of IKE.

Threshold : IPMEIR.TP.IKEV2.98
Upon receipt of a cryptographically protected IKE_AUTH, CREATE_CHILD_SA, or INFORMATIONAL request message with an unfamiliar payload with the Critical Bit set to ONE, IPMEIR devices shall send a corresponding IKE response message with a N(UNSUPPORTED_CRITICAL_PAYLOAD) Payload as the only payload within the Encrypted Payload.

Objective : IPMEIR.TP.IKEV2.99
When narrowing traffic selectors to an acceptable subset of those offered by the initiator but additional subsets are possible for creation of separate CHILD_SAs, IPMEIR devices shall include a N(ADDITIONAL_TS_POSSIBLE) Payload in the CHILD_SA response message.

1.2.3.1 Certificate

Threshold : IPMEIR.TP.IKEV2.CERT.1
IPMEIR shall support certificate data origin authentication.

Threshold : IPMEIR.TP.IKEV2.CERT.3
Upon the receipt of an IKE_SA_INIT request message, IPMEIR devices shall send a Certificate Request Payload in the IKE_SA_INIT response message.

Threshold : IPMEIR.TP.IKEV2.CERT.5
Upon the receipt of an IKE_SA_INIT response message, IPMEIR devices shall send a Certificate Request Payload in the IKE_AUTH request message.

Threshold : IPMEIR.TP.IKEV2.CERT.6
If a Certificate Request Payload is included in the IKE_AUTH request message, IPMEIR devices shall place the Certificate Request Payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.CERT.7
When sending the Certificate Request Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.CERT.7.

Table - IPMEIR.TP.IKEV2.CERT.7

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the Certificate Request Payload as 0x26 (decimal 38).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	variable
Cert Encoding	8-bits	4 decimal
		12 decimal
		13 decimal
Certificate Authority	variable	Per Section 3.7 of RFC 4306

Threshold : IPMEIR.TP.IKEV2.CERT.8
Upon receipt of a Certificate Request Payload in the IKE_SA_INIT response message that identifies a Certification Authority certificate which can be associated with a loaded End Entity certificate, IPMEIR devices shall send a Certificate Payload(s) containing certificate(s) that can be validated to an identified CA in the IKE_AUTH request message.

Threshold : IPMEIR.TP.IKEV2.CERT.9
If a Certificate Payload(s) is included in the IKE_AUTH request message, IPMEIR devices shall place the Certificate Payload(s) within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.CERT.10
Upon receipt of a Certificate Request Payload in the IKE_AUTH request message containing a Certification Authority certificate which can be associated with a loaded End Entity certificate, IPMEIR devices shall send a Certificate Payload(s) in the IKE_AUTH response message.

Threshold : IPMEIR.TP.IKEV2.CERT.11
If a Certificate Payload(s) is included in the IKE_AUTH response message, IPMEIR devices shall place the Certificate Payload(s) within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.CERT.12
When sending multiple Certificate Payloads to provide an End Entity certificate chain, IPMEIR devices shall order the Certificate Payloads such that the first Certificate Payload contains the public key used to sign the Authentication Payload - Authentication Data.

Threshold : IPMEIR.TP.IKEV2.CERT.13
When sending the Certificate Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.CERT.13.

Table - IPMEIR.TP.IKEV2.CERT.13

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the Certificate Request Payload as 0x25 (decimal 37).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	variable
Cert Encoding	8-bits	4 decimal
		12 decimal
		13 decimal
Certificate Data	variable	Per Section 3.6 of RFC 4306

Threshold : IPMEIR.TP.IKEV2.CERT.14
If an End Entity certificate cannot be associated to a Certification Authority certificate, IPMEIR devices shall use Shared Secret data origin authentication (Authentication Method-Shared Key Message Integrity Code).

Threshold : IPMEIR.TP.IKEV2.CERT.15
When using Authentication Method-ECDSA with SHA-256 on the P-256 curve in the IKE_AUTH request Authentication Payload, IPMEIR devices shall calculate the Authentication Data as detailed in RFC 4306 Section 2.15 and RFC 4754 Section 7 and 8.

Threshold : IPMEIR.TP.IKEV2.CERT.16
When using Authentication Method-ECDSA with SHA-256 on the P-256 curve in the IKE_AUTH response Authentication Payload, IPMEIR devices shall calculate the Authentication Data as detailed in RFC 4306 Section 2.15 and RFC 4754 Section 7 and 8.

Threshold : IPMEIR.TP.IKEV2.CERT.17
When using Authentication Method-ECDSA with SHA-384 on the P-384 curve in the IKE_AUTH request Authentication Payload, IPMEIR devices shall calculate the Authentication Data as detailed in RFC 4306 Section 2.15 and RFC 4754 Section 7 and 8.

Threshold : IPMEIR.TP.IKEV2.CERT.18
When using Authentication Method-ECDSA with SHA-384 on the P-384 curve in the IKE_AUTH response Authentication Payload, IPMEIR devices shall calculate the Authentication Data as detailed in RFC 4306 Section 2.15 and RFC 4754 Section 7 and 8.

Threshold : IPMEIR.TP.IKEV2.CERT.19
Upon the receipt of an Authentication Payload containing ECDSA with SHA-256 on the P-256 curve-Authentication Data, IPMEIR devices shall validate the Authentication Data as detailed in RFC 4754 Section 8.

Threshold : IPMEIR.TP.IKEV2.CERT.20
Upon the receipt of an Authentication Payload containing ECDSA with SHA-384 on the P-384 curve-Authentication Data, IPMEIR devices shall validate the Authentication Data as detailed in RFC 4754 Section 8.

Threshold : IPMEIR.TP.IKEV2.CERT.21
Upon the receipt of multiple Certificate Payloads (End Entity certificate chain), IPMEIR devices shall validate the Authentication Payload - Authentication Data using the first Certificate Payload's public key.

Threshold : IPMEIR.TP.IKEV2.CERT.22
Upon the receipt of multiple Certificate Payloads (End Entity certificate chain), IPMEIR devices shall validate the chain of End Entity certificates to ensure that the End Entity certificate chain is validated by a Certification Authority certificate.

Threshold : IPMEIR.TP.IKEV2.CERT.23
If an End Entity certificate received in a Certificate Payload is present in the IPMEIR device's End Entity certificates, IPMEIR devices shall terminate the IKE exchange.

Threshold : IPMEIR.TP.IKEV2.CERT.24
Upon receipt of an End Entity certificate in a Certificate Payload, IPMEIR devices shall validate the signature with a Certification Authority certificate and terminate the IKE exchange if the validation fails.

1.2.3.2 Multiple CHILD_SAs

Objective : IPMEIR.TP.IKEV2.CHILD.1
IPMEIR devices shall support the capability to create a new CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.CHILD.2

When initiating a CREATE_CHILD_SA exchange to create a new CHILD_SA, IPMEIR devices shall format the CREATE_CHILD_SA request message as shown in Table - IPMEIR.TP.IKEV2.CHILD.2.

Table - IPMEIR.TP.IKEV2.CHILD.2

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Per RFC 4306 Section 3.3.1.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Per RFC 4306 Section 3.3.2.
	Attribute Type (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Length (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Value (variable)	Per RFC 4306 Section 3.3.5.
Nonce Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9.

Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.CHILD.3
When responding to a CREATE_CHILD_SA exchange to create a new CHILD_SA, IPMEIR devices shall format the CREATE_CHILD_SA response message as shown in Table - IPMEIR.TP.IKEV2.CHILD.3.

Table - IPMEIR.TP.IKEV2.CHILD.3

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Proposal Number corresponding to selected proposal.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Transform ID corresponding to selected transform.
	Attribute Type (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Length (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Value (variable)	Data Attributes corresponding to selected transform.

Nonce Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9 and negotiated IPMEIR cryptographic suite.
Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.CHILD.4
Upon receipt of a CREATE_CHILD_SA request message to create a new CHILD_SA, if the addition of a new CHILD_SA is not acceptable, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_ADDITIONAL_SAS) Payload as the only payload within the Encrypted Payload as shown in Table - IPMEIR.TP.IKEV2.21.

Threshold : IPMEIR.TP.IKEV2.CHILD.5
When sending a CREATE_CHILD_SA message to create a CHILD_SA, IPMEIR devices shall generate nonces such that the length is at least half the key size of the negotiated pseudo-random function.

Threshold : IPMEIR.TP.IKEV2.CHILD.7
Upon receipt of a CREATE_CHILD_SA request message to create a CHILD_SA, if a proposed cryptographic suite is acceptable but the Diffie-Hellman value received in the Key Exchange Payload was incorrect, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(INVALID_KE_PAYLOAD) Payload as the only payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.CHILD.8
Upon successful completion of a CREATE_CHILD_SA exchange to create a CHILD_SA, IPMEIR devices shall use the new sk_ei/sk_er to protect CHILD_SA traffic on the newly-created CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.CHILD.9
Upon unsuccessful completion of a CREATE_CHILD_SA exchange to create a CHILD_SA, IPMEIR devices shall not tear down the IKE_SA.

1.2.3.3 Cookie Mode

Objective : IPMEIR.TP.IKEV2.CMD.1
IPMEIR devices shall support Cookie Mode.

Threshold : IPMEIR.TP.IKEV2.CMD.2
If the number of half-open IKE_SAs that would trigger Cookie Mode is reached, upon receipt of an IKE_SA_INIT request message with an invalid cookie or no cookie, IPMEIR devices shall send an IKE_SA_INIT response message with a N(COOKIE) Payload as the only payload within the IKE_SA_INIT response message.

Threshold : IPMEIR.TP.IKEV2.CMD.3
When sending the N(COOKIE) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.CMD.3.

Table - IPMEIR.TP.IKEV2.CMD.3

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(COOKIE) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	16 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16390 decimal
Notification Data	64-bits	Per RFC 4306 Section 2.6

Threshold : IPMEIR.TP.IKEV2.CMD.4
If the number of half-open IKE_SAs that would trigger Cookie Mode is reached, upon receipt of an IKE_SA_INIT request message with a valid cookie, IPMEIR devices shall continue processing the rest of the message.

1.2.3.4 Liveness

Objective : IPMEIR.TP.IKEV2.LVNS.1
IPMEIR devices shall support Liveness Test.

Threshold : IPMEIR.TP.IKEV2.LVNS.2
IPMEIR devices shall support the receipt of inbound traffic on the IKE_SA or any CHILD_SA as an indicator of the remote peer's liveness.

Threshold : IPMEIR.TP.IKEV2.LVNS.3
IPMEIR devices shall use empty INFORMATIONAL messages to determine liveness, as described in RFC 4306, Section 2.4.

Threshold : IPMEIR.TP.IKEV2.LVNS.4
If remote peer failure is determined, IPMEIR devices shall not transmit on the IKE_SA and any of its CHILD_SAs.

1.2.3.5 Network Address Translation Traversal

Objective : IPMEIR.TP.IKEV2.NAT-T.1
IPMEIR devices shall support Network Address Translation Traversal (NAT-T).

Threshold : IPMEIR.TP.IKEV2.NAT-T.2
IPMEIR devices shall include a N(NAT_DETECTION_SOURCE_IP) Payload and N(NAT_DETECTION_DESTINATION_IP) Payload in the IKE_SA_INIT request message.

Threshold : IPMEIR.TP.IKEV2.NAT-T.3
When sending the N(NAT_DETECTION_SOURCE_IP) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.NAT-T.3.

Table - IPMEIR.TP.IKEV2.NAT-T.3

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(NAT_DETECTION_SOURCE_IP) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	28 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16388 decimal
Notification Data	160-bits	Per RFC 4306 Section 3.10.1 (NAT_DETECTION_SOURCE_IP)

Threshold : IPMEIR.TP.IKEV2.NAT-T.4
When sending the N(NAT_DETECTION_DESTINATION_IP) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.NAT-T.4.

Table - IPMEIR.TP.IKEV2.NAT-T.4

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(NAT_DETECTION_DESTINATION_IP) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	28 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16389 decimal
Notification Data	160-bits	Per RFC 4306 Section 3.10.1 (NAT_DETECTION_DESTINATION_IP)

Threshold : IPMEIR.TP.IKEV2.NAT-T.5
Upon the receipt of a N(NAT_DETECTION_SOURCE_IP) Payload and N(NAT_DETECTION_DESTINATION_IP) Payload, IPMEIR devices shall include a N(NAT_DETECTION_SOURCE_IP) Payload and N(NAT_DETECTION_DESTINATION_IP) Payload in the IKE_SA_INIT response message.

Threshold : IPMEIR.TP.IKEV2.NAT-T.6
When receiving N(NAT_DETECTION_SOURCE_IP) Payload, IPMEIR devices shall compare the hash contents of the N(NAT_DETECTION_SOURCE_IP) Payload with a hash calculated using the IKE_SA Initiator's SPI, the IKE_SA Responder's SPI, the CT address and port of the remote IPMEIR device's interface used in the IKE negotiation as input; IPMEIR devices shall mark the IKE_SA as requiring NAT-T if the comparison of the N(NAT_DETECTION_SOURCE_IP) Payload hash with the locally generated hash results in a mismatch.

Threshold : IPMEIR.TP.IKEV2.NAT-T.7
When receiving N(NAT_DETECTION_DESTINATION_IP) Payload, IPMEIR devices shall compare the hash contents of the N(NAT_DETECTION_DESTINATION_IP) Payload with a hash calculated using the IKE_SA Initiator's SPI, the IKE_SA Responder's SPI, the CT address and port of the local interface used in the IKE negotiation as input; IPMEIR devices shall mark the IKE_SA as requiring NAT-T if the comparison of the N(NAT_DETECTION_DESTINATION_IP) Payload hash with the locally generated hash results in a mismatch.

Threshold : IPMEIR.TP.IKEV2.NAT-T.9
When NAT is detected, IPMEIR devices shall format the IKE message UDP header as detailed in the Table IPMEIR.TP.IKEV2.NAT-T.9.

Table - IPMEIR.TP.IKEV2.NAT-T.9

Field	Size	Value
Source Port	16-bits	4500 decimal
Destination Port	16-bits	Initiator = 4500 decimal
		Responder = Variable
Length	16-bits	The length in octets of this datagram including this header and the data.
Checksum	16-bits	Per RFC 3948 Section 2.2.
Non-ESP Marker	32-bits	0 decimal. Per RFC 4306 Section 2.23 and RFC 3948 Section 2.2.

Objective : IPMEIR.TP.IKEV2.NAT-T.10
When a NAT device has been detected, the IPMEIR device behind the NAT shall initiate sending NAT-Keepalive packets.

Threshold : IPMEIR.TP.IKEV2.NAT-T.11
IPMEIR devices shall format NAT-Keepalive packets as detailed in Table IPMEIR.TP.IKEV2.NAT-T.11.

Table - IPMEIR.TP.IKEV2.NAT-T.11

Field	Size	Value
Source Port	16-bits	Same as used by UDP-ESP encapsulation.
Destination Port	16-bits	Same as used by UDP-ESP encapsulation.
Length	16-bits	The length in octets of this datagram including this header and the data.
Checksum	16-bits	Set to ZERO (0).
Keepalive	8-bits	0xFF

1.2.3.6 Orphan Security Association Recovery

Threshold : IPMEIR.TP.IKEV2.ORPHRC.1
IPMEIR devices shall support Orphan SA Recovery.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.2
Upon receipt of a cryptographically protected IKE request message with unknown IKE SPIs, IPMEIR devices shall send an one-way INFORMATIONAL response message with an N(INVALID_IKE_SPI) Payload.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.3
IPMEIR devices shall format the one-way INFORMATIONAL response message with a N(INVALID_IKE_SPI) Payload as shown in Table - IPMEIR.TP.IKEV2.ORPHRC.3.

Table - IPMEIR.TP.IKEV2.ORPHRC.3

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Populated with the received IKE request's (i.e. the IKE request message with unknown IKE SPIs) IKE_SA Initiator's SPI Field.
	IKE_SA Responder's SPI (64-bits)	Populated with the received IKE request's (i.e. the IKE request message with unknown IKE SPIs) IKE_SA Responder's SPI Field.
	Next Payload (8-bits)	41 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	37 decimal
	Flags (8-bits)	0010X000 (binary) where X is the inverted IKE request's (i.e. the IKE request message with unknown IKE SPIs) Initiator Bit.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Populated with the received IKE request's (i.e. the IKE request message with unknown IKE SPIs) Message ID.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Notify Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Protocol ID (8-bits)	1 decimal
	SPI Size (8-bits)	0 decimal
	Notify Message Type (16-bits)	4 decimal

Threshold : IPMEIR.TP.IKEV2.ORPHRC.4
Upon receipt of a cryptographically protected IKE response message with unknown IKE SPIs, IPMEIR devices shall discard that IKE response message.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.5
Upon receipt of an one-way INFORMATIONAL response message with a N(INVALID_IKE_SPI) Payload, IPMEIR devices shall send an empty INFORMATIONAL request message on the IKE_SA indicated by the IKE SPIs in the IKE Header of the one-way INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.6
Upon receipt of a cryptographically protected ESP packet with an unknown SPI, if an IKE_SA does not exist with the peer, IPMEIR devices shall send an one-way INFORMATIONAL request message with a N(INVALID_SPI) Payload.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.7
IPMEIR devices shall format the one-way INFORMATIONAL request message with a N(INVALID_SPI) Payload as shown in Table - IPMEIR.TP.IKEV2.ORPHRC.7.

Table - IPMEIR.TP.IKEV2.ORPHRC.7

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	0 decimal
	IKE_SA Responder's SPI (64-bits)	0 decimal
	Next Payload (8-bits)	41 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	37 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit set to 0.
		V = Version Bit
		I = Initiator Bit set to 1.
	Message ID (32-bits)	0 decimal
	Length (32-bits)	Per RFC 4306 Section 3.1.
Notify Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	4 decimal
	Notify Message Type (16-bits)	11 decimal
	Notification Data (32-bits)	Populated with the received ESP packet's (i.e. the ESP packet with an unknown SPI) SPI.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.8
Upon receipt of an one-way INFORMATIONAL request message with a N(INVALID_SPI) Payload, IPMEIR devices shall send an empty INFORMATIONAL request message on the IKE_SA parenting the CHILD_SA as indicated by the SPI in the Notification Data of the one-way INFORMATIONAL request message and the source address of the peer that sent the one-way INFORMATIONAL request message.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.9
Upon receipt of traffic to be sent on a CHILD_SA to a remote peer that has been deemed failed, IPMEIR devices shall attempt to establish a new equivalent IKE_SA and CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.10
Upon receipt of a cryptographically protected ESP packet with an unknown SPI, if an IKE_SA exists with the peer, IPMEIR devices shall send an INFORMATIONAL request message with a N(INVALID_SPI) Payload on the IKE_SA.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.11
When sending the N(INVALID_SPI) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.ORPHRC.11.

Table - IPMEIR.TP.IKEV2.ORPHRC.11

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the IKE Header preceding the N(INVALID_SPI) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	Per RFC 4306 Section 3.2.
Protocol ID	8-bits	3 decimal
SPI Size	8-bits	4 decimal
Notify Message Type	16-bit	11 decimal
Notification Data	32-bits	Populated with the received ESP packet's (i.e. the ESP packet with an unknown SPI) SPI.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.12
Upon receipt of an INFORMATIONAL request message with a N(INVALID_SPI) Payload on an IKE_SA, IPMEIR devices shall send an empty INFORMATIONAL response message.

Threshold : IPMEIR.TP.IKEV2.ORPHRC.13
Upon receipt of an INFORMATIONAL request message with a N(INVALID_SPI) Payload on an IKE_SA, IPMEIR devices shall locally delete the CHILD_SA as indicated by the SPI in the Notification Data of the N(INVALID_SPI) Payload.

1.2.3.7 REKEY

Objective : IPMEIR.TP.IKEV2.REKEY.1
IPMEIR devices shall support the capability to rekey an SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.2

When initiating a CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall format the CREATE_CHILD_SA request message as shown in Table - IPMEIR.TP.IKEV2.REKEY.2.

Table - IPMEIR.TP.IKEV2.REKEY.2

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Per RFC 4306 Section 3.3.1.
	Protocol ID (8-bits)	1 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (64-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Per RFC 4306 Section 3.3.2.
	Attribute Type (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Length (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Value (variable)	Per RFC 4306 Section 3.3.5.
Nonce Payload	Next Payload (8-bits)	34 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9.

Key Exchange Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Diffie-Hellman Group Number (16-bits)	Per RFC 4306 Section 3.4.
	RESERVED (16-bits)	0 decimal
	Key Exchange Data (variable)	Per RFC 4306 Section 3.4.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.REKEY.3

After rekeying an IKE_SA, IPMEIR devices shall format the CREATE_CHILD_SA response message as shown in Table - IPMEIR.TP.IKEV2.REKEY.3.

Table - IPMEIR.TP.IKEV2.REKEY.3

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Proposal Number corresponding to selected proposal.
	Protocol ID (8-bits)	1 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (64-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Transform ID corresponding to selected transform.
	Attribute Type (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Length (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Value (variable)	Data Attributes corresponding to selected transform.

Nonce Payload	Next Payload (8-bits)	34 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9 and negotiated IPMEIR cryptographic suite.
Key Exchange Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Diffie-Hellman Group Number (16-bits)	Diffie-Hellman Group Number corresponding to selected Diffie-Hellman group.
	RESERVED (16-bits)	0 decimal
	Key Exchange Data (variable)	Per RFC 4306 Section 3.4 and negotiated IPMEIR cryptographic suite.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.REKEY.4
After a successful CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall generate SKEYSEED as detailed in RFC 4306 Section 2.18.

Threshold : IPMEIR.TP.IKEV2.REKEY.5
After a successful CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall set the Message IDs (Local Message ID - the Message ID it would use for sending a request message to a peer and the Remote Message ID - the Message ID it would expect to receive from a peer request message) of the rekeyed IKE_SA to ZERO.

Threshold : IPMEIR.TP.IKEV2.REKEY.6
After a successful CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall set the Window Size to ONE.

Threshold : IPMEIR.TP.IKEV2.REKEY.7
After a successful CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall delete the old IKE_SA within the IKE_SA used for the IKE_SA rekey; the peer that initiates the INFORMATIONAL exchange with the Delete Payload is the peer that initiated the successful IKE_SA rekey.

Threshold : IPMEIR.TP.IKEV2.REKEY.8
Upon receipt of an INFORMATIONAL request message with a Delete Payload to delete an IKE_SA that has been rekeyed, IPMEIR devices shall mark all CHILD_SAs parented by the old IKE_SA as being parented by the rekeyed IKE_SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.9
Upon receipt of an INFORMATIONAL response message with a Delete Payload to delete an IKE_SA that has been rekeyed, IPMEIR devices shall mark all CHILD_SAs parented by the old IKE_SA as being parented by the rekeyed IKE_SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.10

When initiating a CREATE_CHILD_SA exchange to rekey a CHILD_SA, IPMEIR devices shall format the CREATE_CHILD_SA request message as shown in Table - IPMEIR.TP.IKEV2.REKEY.10.

Table - IPMEIR.TP.IKEV2.REKEY.10

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 2.2 and 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	41 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Notify Payload (REKEY_SA)	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	4 decimal
	Notify Message Type (16-bits)	16393 decimal
	SPI (32-bits)	Per RFC 4306 Section 3.10; SPI of inbound CHILD_SA to be rekeyed.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Per RFC 4306 Section 3.3.1.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.

Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Per RFC 4306 Section 3.3.2.
	Attribute Type (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Length (16-bits)	Per RFC 4306 Section 3.3.5.
	Attribute Value (variable)	Per RFC 4306 Section 3.3.5.
Nonce Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9.
Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.REKEY.11

After rekeying an CHILD_SA, IPMEIR devices shall format the CREATE_CHILD_SA response message as shown in Table - IPMEIR.TP.IKEV2.REKEY.11.

Table - IPMEIR.TP.IKEV2.REKEY.11

Header/Payload/Substructure	Field (size in bits)	Value
IKE Header	IKE_SA Initiator's SPI (64-bits)	Per RFC 4306 Section 3.1.
	IKE_SA Responder's SPI (64-bits)	Per RFC 4306 Section 3.1.
	Next Payload (8-bits)	46 decimal
	Major Version (4-bits)	2 decimal
	Minor Version (4-bits)	0 decimal
	Exchange Type (8-bits)	36 decimal
	Flags (8-bits)	Per RFC 4306 Section 3.1.
		Flags Field Format = XXRVIXXX
		X = RESERVED
		R = Response Bit
		V = Version Bit
		I = Initiator Bit
	Message ID (32-bits)	Per RFC 4306 Section 3.1.
	Length (32-bits)	Per RFC 4306 Section 3.1.
Encrypted Payload Header	Next Payload (8-bits)	33 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Initialization Vector (variable)	Per negotiated IPMEIR cryptographic suite.
Security Association Payload	Next Payload (8-bits)	40 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
Proposal Substructure	0 (last) or 2 (8-bits)	Per RFC 4306 Section 3.3.1.
	RESERVED (8-bits)	0 decimal
	Proposal Length (16-bits)	Per RFC 4306 Section 3.3.1.
	Proposal Number (8-bits)	Proposal Number corresponding to selected proposal.
	Protocol ID (8-bits)	3 decimal
	SPI Size (8-bits)	Per RFC 4306 Section 3.3.1
	Number of Transforms (8-bits)	Per RFC 4306 Section 3.3.1.
	SPI (32-bits)	Per RFC 4306 Section 3.3.1.
Transform Substructure	0 (last) or 3 (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform Length (16-bits)	Per RFC 4306 Section 3.3.2.
	Transform Type (8-bits)	Per RFC 4306 Section 3.3.2.
	RESERVED (8-bits)	0 decimal
	Transform ID (16-bits)	Transform ID corresponding to selected transform.
	Attribute Type (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Length (16-bits)	Data Attributes corresponding to selected transform.
	Attribute Value (variable)	Data Attributes corresponding to selected transform.

Nonce Payload	Next Payload (8-bits)	44 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Nonce Data (variable)	Per RFC 4306 Section 3.9 and negotiated IPMEIR cryptographic suite.
Traffic Selector Initiator Payload	Next Payload (8-bits)	45 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Traffic Selector Responder Payload	Next Payload (8-bits)	0 decimal
	Critical Bit (1-bit)	0 decimal
	RESERVED (7-bits)	0 decimal
	Payload Length (16-bits)	Per RFC 4306 Section 3.2.
	Number of TSs (8-bits)	Per RFC 4306 Section 3.13.
	RESERVED (24-bits)	0 decimal
	Traffic Selectors (variable)	Per RFC 4306 Section 2.9 and Section 3.13.1 and RFC 4718 Section 4.10.
Encrypted Payload Trailer	Padding (variable)	Per RFC 4306 Section 3.14.
	Pad Length (8-bits)	Per RFC 4306 Section 3.14.
	Integrity Checksum Data (variable)	Per negotiated IPMEIR cryptographic suite.

Threshold : IPMEIR.TP.IKEV2.REKEY.12
When sending a CREATE_CHILD_SA message to rekey a CHILD_SA, IPMEIR devices shall generate nonces such that the length is at least half the key size of the negotiated pseudo-random function.

Threshold : IPMEIR.TP.IKEV2.REKEY.13
When sending a CREATE_CHILD_SA message to rekey an IKE_SA, IPMEIR devices shall generate nonces such that the length is at least half the key size of the negotiated pseudo-random function of the old IKE_SA and at least half the key size of the largest proposed pseudo-random function in the Security Association Payload.

Threshold : IPMEIR.TP.IKEV2.REKEY.14
After initiating a successful CREATE_CHILD_SA exchange to rekey a CHILD_SA, IPMEIR devices shall delete the old CHILD_SA; the peer that initiates the INFORMATIONAL exchange with the Delete Payload is the peer that initiated the successful CHILD_SA rekey.

Threshold : IPMEIR.TP.IKEV2.REKEY.16
Upon the establishment of redundant IKE_SAs after concurrent IKE_SA rekeys, if the rekeyed IKE_SA with the lowest nonce was created by it, IPMEIR devices shall initiate an INFORMATIONAL exchange to delete that redundant IKE_SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.18
Upon receipt of a CREATE_CHILD_SA request message to rekey an SA, if a proposed cryptographic suite is acceptable but the Diffie-Hellman value received in the Key Exchange Payload was incorrect, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(INVALID_KE_PAYLOAD) Payload as the only payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.REKEY.19
Upon successful completion of a CREATE_CHILD_SA exchange to rekey an IKE_SA, IPMEIR devices shall use the new sk_ei/sk_er to protect IKE_SA traffic on the newly-created IKE_SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.20
Upon successful completion of a CREATE_CHILD_SA exchange to rekey a CHILD_SA, IPMEIR devices shall use the new sk_ei/sk_er to protect CHILD_SA traffic on the newly-created CHILD_SA.

Threshold : IPMEIR.TP.IKEV2.REKEY.22
Upon receipt of a CREATE_CHILD_SA request message to rekey a CHILD_SA that does not exist or the IPMEIR device is in process of deleting, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_PROPOSAL_CHOSEN) Payload as the only payload within the Encrypted Payload of the CREATE_CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.REKEY.24
Upon receipt of a CREATE_CHILD_SA request message to rekey an IKE_SA that the IPMEIR device is in process of deleting, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_PROPOSAL_CHOSEN) Payload as the only payload within the Encrypted Payload of the CREATE_CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.REKEY.25
Upon receipt of an INFORMATIONAL request message with a Delete Payload to delete a CHILD_SA(s) and the IPMEIR device is in the process of rekeying the IKE_SA, IPMEIR devices shall send an INFORMATIONAL response message without a corresponding Delete Payload(s).

Threshold : IPMEIR.TP.IKEV2.REKEY.26
Upon receipt of a CREATE_CHILD_SA request message to create or rekey a CHILD_SA and the IPMEIR device is in the process of rekeying the IKE_SA, IPMEIR devices shall send a CREATE_CHILD_SA response message with a N(NO_ADDITIONAL_SAS) Payload as the only payload within the Encrypted Payload of the CREATE_CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.REKEY.27
Upon receipt of a CREATE_CHILD_SA request message to rekey an IKE_SA, IPMEIR devices must not accept a proposal with a value of "NONE" for the Diffie-Hellman transform.

Threshold : IPMEIR.TP.IKEV2.REKEY.28
When including a KE Payload in a CREATE_CHILD_SA Request message to rekey an SA, the Initiator must use the same random ECP group as was used in the IKE_SA_INIT.

1.2.3.8 Transport Mode

Objective : IPMEIR.TP.IKEV2.TRPMD.1
IPMEIR devices shall support the negotiation of ESPv3 Transport Mode CHILD_SAs.

Threshold : IPMEIR.TP.IKEV2.TRPMD.2
When negotiating Transport Mode for a CHILD_SA, IPMEIR devices shall include a N(USE_TRANSPORT_MODE) Payload in the CHILD_SA request message within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.TRPMD.3
If local policy supports negotiation of Transport Mode, upon receipt of a CHILD_SA request message with a N(USE_TRANSPORT_MODE) Payload, IPMEIR devices shall include a N(USE_TRANSPORT_MODE) Payload in the CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.TRPMD.4
If local policy does not support negotiation of Transport Mode, upon receipt of a CHILD_SA request message with a N(USE_TRANSPORT_MODE) Payload, IPMEIR devices shall not include a N(USE_TRANSPORT_MODE) Payload in the CHILD_SA response message.

Threshold : IPMEIR.TP.IKEV2.TRPMD.5
If local policy only supports negotiation of a Transport Mode CHILD_SA, upon receipt of a CHILD_SA request message without a N(USE_TRANSPORT_MODE) Payload, IPMEIR devices shall send a CHILD_SA response message with a N(NO_PROPOSAL_CHOSEN) Payload as the only payload within the Encrypted Payload.

Threshold : IPMEIR.TP.IKEV2.TRPMD.6
If a N(USE_TRANSPORT_MODE) Payload was sent in the CHILD_SA request message but not received in a CHILD_SA response message and local policy does not support negotiation of a Tunnel Mode CHILD_SA, IPMEIR devices shall delete the CHILD_SA that was established in Tunnel Mode.

Threshold : IPMEIR.TP.IKEV2.TRPMD.7
When sending the N(USE_TRANSPORT_MODE) Payload, IPMEIR devices shall format the payload as detailed in Table - IPMEIR.TP.IKEV2.TRPMD.7.

Table - IPMEIR.TP.IKEV2.TRPMD.7

Field	Size	Value
Next Payload	8-bits	Per RFC 4306 Section 3.2. IPMEIR devices shall code the Next Payload field of the payload (or the IKE Header) preceding the N(USE_TRANSPORT_MODE) Payload as 0x29 (decimal 41).
Critical Bit	1-bit	0 decimal
RESERVED	7-bits	0 decimal
Payload Length	16-bits	8 decimal
Protocol ID	8-bits	0 decimal
SPI Size	8-bits	0 decimal
Notify Message Type	16-bit	16391 decimal

1.2.3.8.1 Network Address Translation Traversal

Threshold : IPMEIR.TP.IKEV2.TRPMD.NAT-T.1
When negotiating Transport Mode CHILD_SAs when NAT is detected, IPMEIR devices shall send a Traffic Selector - Initiator Payload containing one address, the local host IP address.

Threshold : IPMEIR.TP.IKEV2.TRPMD.NAT-T.2
When negotiating Transport Mode CHILD_SAs when NAT is detected, IPMEIR devices shall send a Traffic Selector - Responder Payload containing one address, the remote host IP address.

Appendix A References

Identifier	Title
RFC768	User Datagram Protocol
RFC791	INTERNET PROTOCOL
RFC792	INTERNET CONTROL MESSAGE PROTOCOL
RFC2460	Internet Protocol, Version 6 (IPv6) Specification
RFC2461	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462	IPv6 Stateless Address Autoconfiguration
RFC2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC3948	UDP Encapsulation of IPsec ESP Packets
RFC4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC4306	Internet Key Exchange (IKEv2) Protocol
RFC4718	IKEv2 Clarifications and Implementation Guidelines
RFC4754	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
RFC4869	Suite B Cryptographic Suites for IPsec
RFC5759	Suite B Certificate and Certificate Revocation List (CRL) Profile
Elliptic Curve Cryptography Groups IPMEIR IS	A supplemental technical reference for IPMEIR IS.