IPv6 Conformance

Test Specification
IKEv1
SGW using Main Mode

Technical Document

Revision 1.0

IPv6 Forum
IPv6 Logo Committee

Modification Record

Version 1.0 April 21, 2006

Acknowledgement

IPv6 Forum would like to acknowledge the efforts of the following organizations in the development of this test specification.

- TAHI Project
- IRISA
- University of New Hampshire - Interoperability Laboratory (UNH-IOL)

Introduction

The IPv6 forum plays a major role in bringing together industrial actors, to develop and deploy the next generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community.

Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products. To avoid confusion in the mind of customers, a globally unique logo program should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo program will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase 1 :

In a first stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.

Phase 2 :

The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

To avoid confusion, the logo "IPv6 Ready" will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.

Phase 3 :

Same as Phase 2 with IPsec mandated.

Requirements

The Node Under Test (NUT) must satisfy following requirements.

parameter			BASIC	ADVANCED
Exchange type	Phase-1		Main mode	Aggressive mode
	Phase-2		Quick mode	–
ISAKMP SA	Encryption Algorithm *1		3DES-CBC	DES-CBC, AES-CBC (128bit)
	Hash Algorithm		SHA1	MD5
	Authentication Method		Pre-shared key	Digital Signature (RSA)
	Diffie-Hellman Group		2	1,5,14
	Life Type		Seconds	–
IPsec SA	Encapsulation mode	End-Node	Transport	Tunnel
		SGW	Tunnel	–
	Security Protocol		ESP with Authentication	ESP (without Authentication)
	Encryption Algorithm		3DES-CBC	DES-CBC, AES-CBC (128bit), ESP-NULL
	Hash Algorithm		HMAC-SHA1	HMAC-MD5 , AES-XCBC
	Life Type		Seconds	–
IKE Phase-1	Sending multiple proposal		–	Support
IKE Phase-2	PFS		–	Support
	Commit bit		–	Support
	Re-key		Support	–
	Sending multiple proposal		–	Support

IPsec Transmission	Encapsulation mode	End-Node	Transport	Tunnel
		SGW	Tunnel	-
	Security Protocol		ESP with Authentication	ESP (without Authentication)
	Encryption Algorithm		3DES-CBC	DES-CBC, AES-CBC (128bit), ESP-NULL
	Hash Algorithm		HMAC-SHA1	HMAC-MD5 , AES-XCBC
	Anti-replay		Sender	Receiver

Equipment Type:

We define two possibilities for equipment types, they are as follows:

End-Node:

A node who can use IKE(IPsec) only for itself. Host and Router can be an End-Node.

SGW (Security Gateway):

A node who can provide IKE(IPsec tunnel mode) for nodes behind it. Router can be a SGW.

Category:

All NUTs are required to support BASIC. ADVANCED is required for all NUTs which support ADVANCED function.

References

This test specification focus on following IKE related RFCs.

RFC2406 : IP Encapsulating Security Payload (ESP)

RFC2407 : The Internet IP Security Domain of Interpretation for ISAKMP

RFC2408 : Internet Sesurity Association and Key Management Protocol (ISAKMP)

RFC2409 : The Internet Key Exchange (IKE)

RFC3526 : More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)

RFC3566 : The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec

RFC3602 : The AES-CVC Cipher Algorithm and Its Use with IPsec

RFC4109 : Algorithms for Internet Key Exchange version 1 (IKEv1)

---TOC---

1. Test Details

This chapter contains detailed information, including terminology, which is described below.

Terminology:

TN : Tester Node
NUT : Node Under Test (Target Implementation)
SGW : Security Gateway

Required Application:

All tests use ICMP Echo Request and Echo Reply messages by default. ICMP is independent from any implemented application and this adds clarity to the test. If the NUT can not apply IPsec for ICMPv6 packets, it is acceptable to use other protocols rather than ICMPv6. In this case, the device must support either ICMPv6, TCP or UDP. The application and port number are unspecified when TCP or UDP packets are used. The test coordinator should support any ports associated with an application used for the test. Applicants must mention the specific protocol and port that was used to execute the tests.

Topology:

In "2 Common Topology" the network topology for the test is shown.

2. Common Topology

- Initiator Test

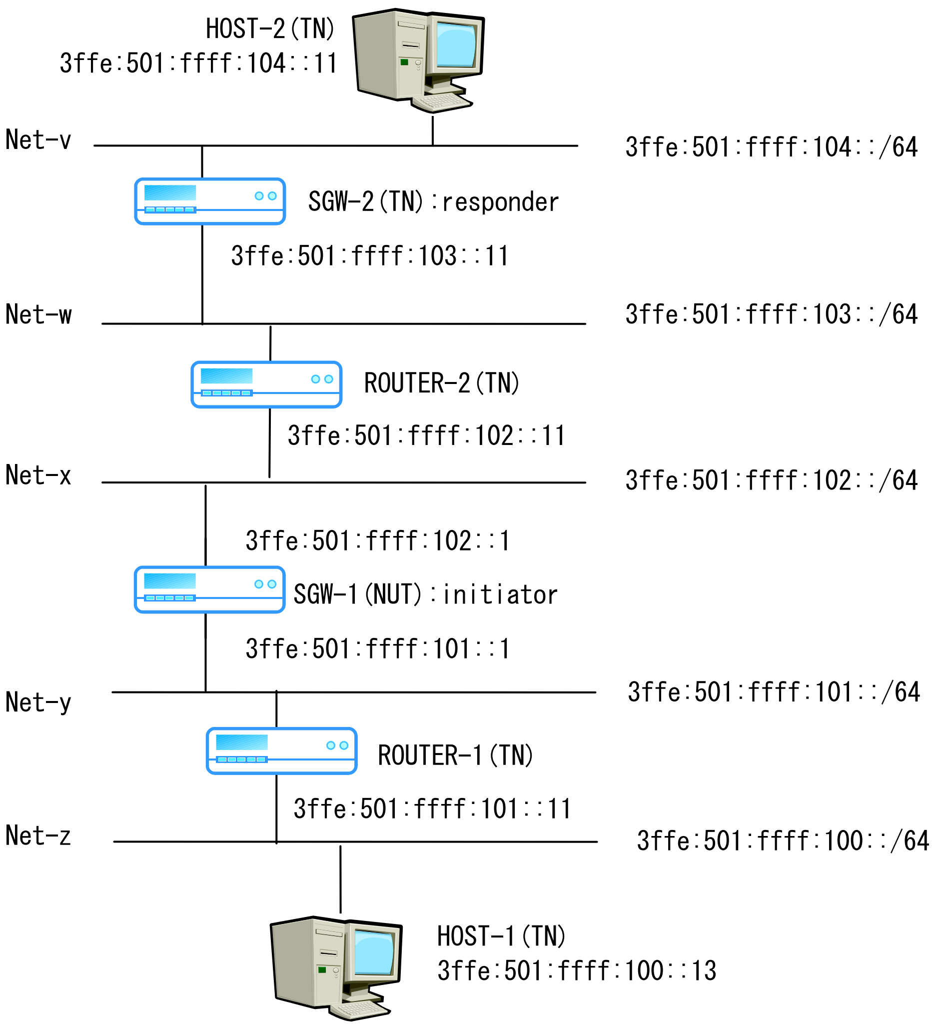

Figure 1 Topology for SGW vs. SGW (Initiator Test)

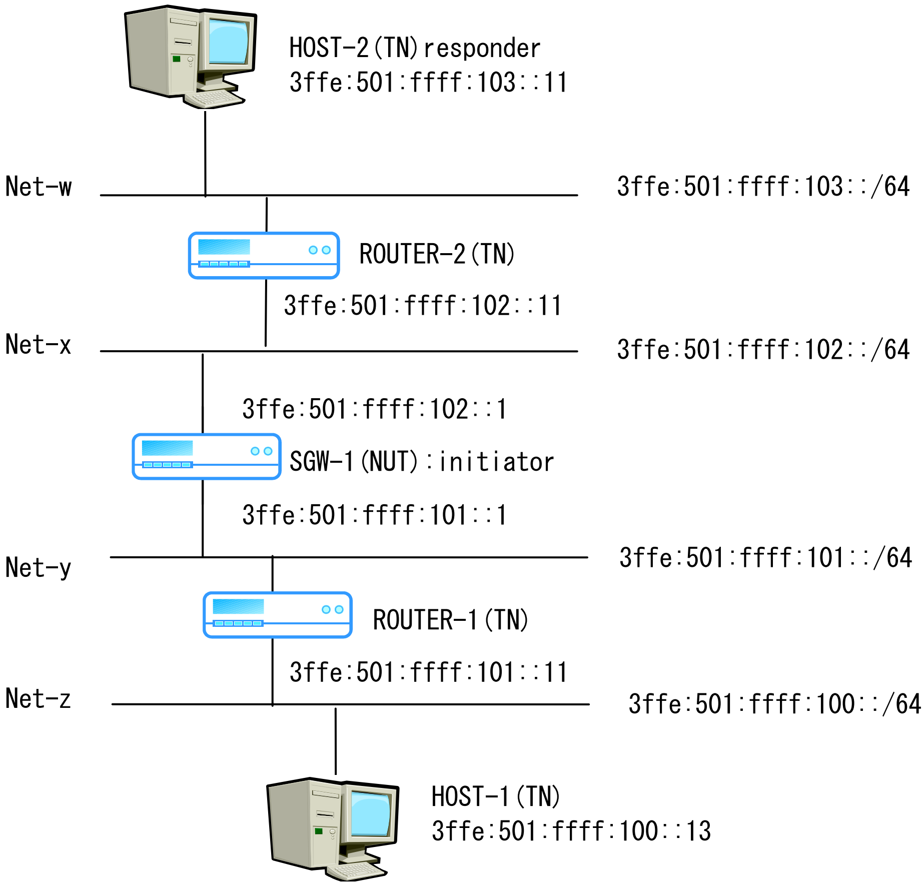

Figure 2 Topology for SGW vs. HOST (Initiator Test)

- Responder Test

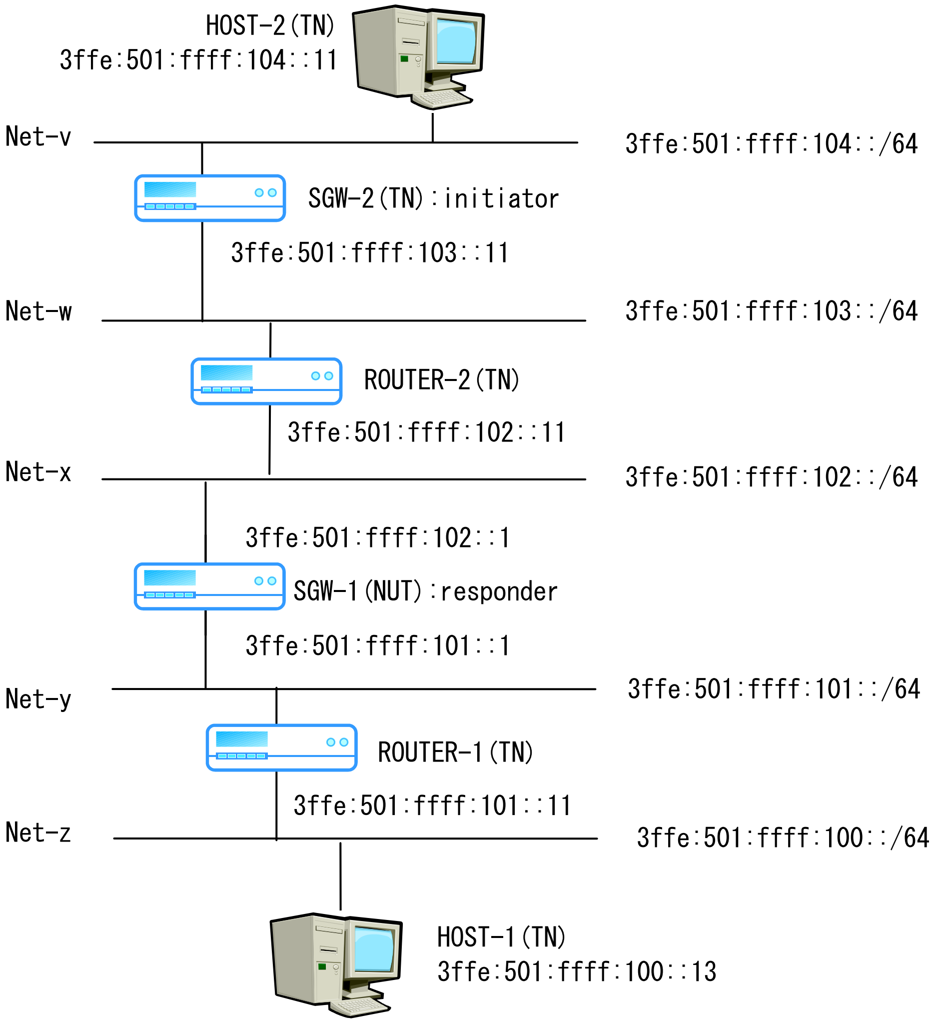

Figure 3 Topology for SGW vs. SGW (Responder Test)

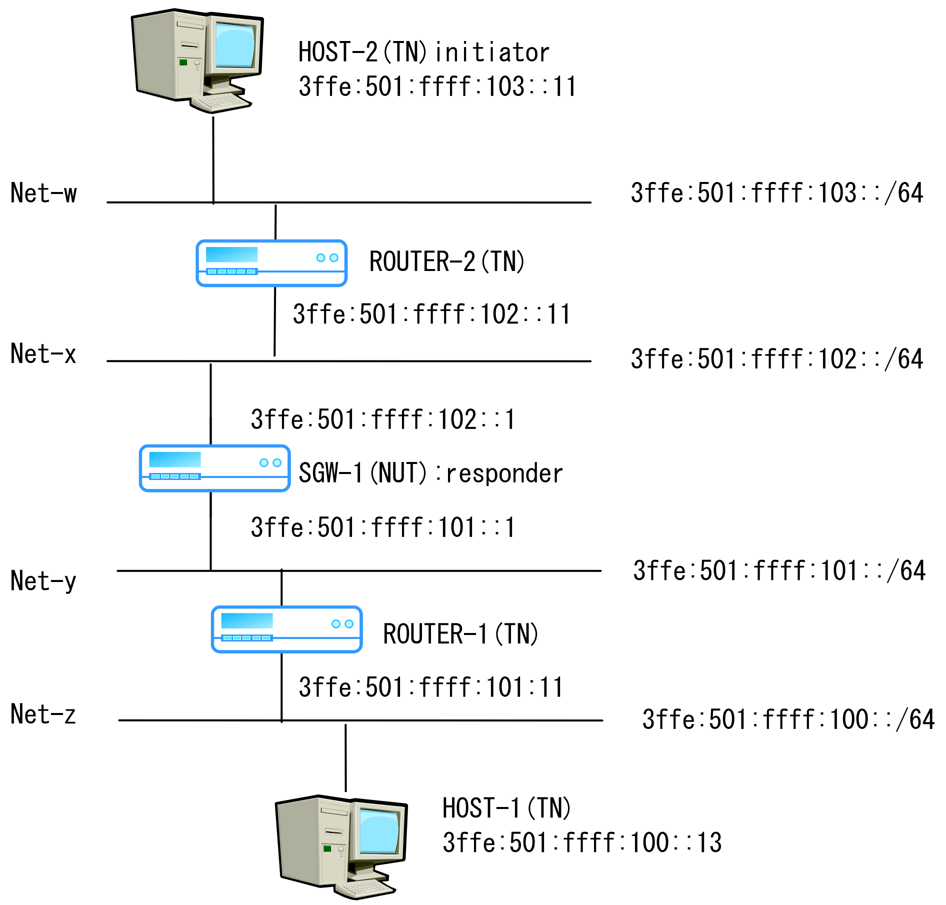

Figure 4 Topology for SGW vs. HOST (Responder Test)

3. Common Configuration

Phase-1:

Table 1. Phase-1 Common Configuration

Machine	Src	Dest	Phase II							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

Phase-2:

Table 2. Phase-2 Common Configuration

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

4 Common Sequence

As a preparation test sequence, the following Identity Protection or Aggressive exchanges are executed before the Phase-2 test is executed.

4.1 Phase-1 Sequence (Initiator Test)

* Identity Protection Exchange

```
          <IDENTITY PROTECTION EXCHANGE>

 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
(6)                      <========      HDR*; IDir; HASH_R
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

*** Aggressive Exchange**

```
                         <AGGRESSIVE EXCHANGE>

 #     Initiator(NUT)    Direction      Responder(TN)       NOTE
(1)  HDR; SA; KE;          =>                          Begin ISAKMP-SA or
                                                       Proxy negotiation
     NONCE; IDii                                       and Key Exchange
(2)                        <=           HDR; SA; KE;
                                       NONCE; IDir; AUTH
                                                       Initiator Identity
                                                       Verified by Responder
                                                       Key Generated
                                                       Basic SA agreed upon
(3)  HDR*; AUTH            =>
                                                       Responder Identity
                                                       Verified by Initiator
                                                       SA established
```

1. Recieve the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). There can be only one Proposal and one Transform offered (i.e. no choices) in order for the aggressive exchange to work. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Random information provided by both parties SHOULD be used by the authentication mechanism to provide shared proof of participation in the exchange. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Random information provided by both parties SHOULD be used by the authentication mechanism to provide shared proof of participation in the exchange. Additionally, the responder transmits identification information.

All of this information is transmitted under the protection of the agreed upon authentication function. Local security policy dictates the action of the responder if no proposed protection suite is accepted. One possible action is the transmission of a Notify payload as part of an Informational Exchange.

3. Recieve the third message from NUT
   In the third (3) message, the initiator transmits the results of the agreed upon authentication function. This information is transmitted under the protection of the common shared secret. Local security policy dictates the action if an error occurs during these messages. One possible action is the transmission of a Notify payload as part of an Informational Exchange.

4.2 Phase-1 Sequence (Responder Test)

* Identity Protection Exchange

```
          <IDENTITY PROTECTION EXCHANGE>

#   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========      HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
(6)                      <========     HDR*; IDir; HASH_R
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

* Aggressive Exchange

```
                        <AGGRESSIVE EXCHANGE>
 #      Initiator(TN)    Direction      Responder(NUT)       NOTE
(1)   HDR; SA; KE;         =>                             Begin ISAKMP-SA or
                                                          Proxy negotiation
      NONCE; IDii                                         and Key Exchange
(2)                        <=         HDR; SA; KE;
                                      NONCE; IDir; AUTH
                                                          Initiator Identity
                                                          Verified by Responder
                                                          Key Generated
                                                          Basic SA agreed upon
(3)   HDR*; AUTH           =>
                                                          Responder Identity
                                                          Verified by Initiator
                                                          SA established
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). There can be only one Proposal and one Transform offered (i.e. no choices) in order for the aggressive exchange to work. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Random information provided by both parties SHOULD be used by the authentication mechanism to provide shared proof of participation in the exchange. Additionally, the initiator transmits identification information.

2. Recieve the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Random information provided by both parties SHOULD be used by the authentication mechanism to provide shared proof of participation in the exchange. Additionally, the responder transmits identification information. All of this information is transmitted under the protection of the agreed upon authentication function. Local security policy dictates the action of the responder if no proposed protection suite is accepted. One possible action is the transmission of a Notify payload as part of an Informational Exchange.

3. Send the third message from TN
   In the third (3) message, the initiator transmits the results of the agreed upon authentication function. This information is transmitted under the protection of the common shared secret. Local security policy dictates the action if an error occurs during these messages. One possible action is the transmission of a Notify payload as part of an Informational Exchange.

5. Terminology

Generic:

SGW:	Security Gateway
End-Node:	End Node
Initiator:	Initiator of IKE
Responder:	Responder of IKE

Configuration Table:

Ex Mode:	Exchange mode(Aggresive mode can also be chosen as Ex Mode)
IDx:	identity payload(FQDN or user FQDN can also be chosen as IDx)
IDci:	identity payload
IDcr:	identity payload
Enc Alg:	IKE Encryption Algorithm
Hash Alg:	IKE Authentication Algorithm
Key Value:	pre-shared key value
PH1 Lt:	Phase-1 Lifetime
PH2 Lt:	Phase-2 Lifetime
Proto ID:	Protocol Identifier
Trans ID:	Transform Identifier
Mode:	Encapsulation Mode
Auth Alg:	Authentication Algorithm
Auth Method:	Authentication Method
DH Group:	Diffie-Hellman Group
Upper:	Upper Layer Protocol
SGW-1 addr;	SGW-1 address
SGW-2 addr:	SGW-2 address
Net-z:	Net-z network address
Net-v:	Net-v network address

6. Description

Each test specification consists of following parts.

Purpose:	The Purpose is the short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the future or capability to be tested.
Category:	The Category shows what classification of device must satisfy the test.
Initialization:	The Initialization describes how to initialize and configure the NUT before starting each test. If a value is not provided, then the protocol’s default value is used.
Procedure:	The Procedure describes step-by-step instructions for carrying out the test.
Judgment:	The Judgment describes expected result. If we can observe as same result as the description of Judgment, the NUT passes the test.
References:	The References section contains some parts of specification

7. SGW Test

This Chapter describes the test specification for SGW using Main Mode.

7.1. Architecture

Scope:
Following tests focus on Internet Key Exchange Architecture.

Overview:
Tests in this section verify that a node properly process and transmit based on the Internet Key Exchange specification for SGW.

7.1.1 ISAKMP Header format

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Initiator cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 1(Security Association Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  indicates the type of exchange being used.
  (In this test, this field is set as 2(main mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission.
  |0|0|0|0|0|A|C|E|
- Message ID field
  During Phase 1 negotiations, the value MUST be set to 0.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- Termination
  Clean up SAD and SPD

Judgment:

The first message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).(cookie is set to Initiator cookie filed,Major version=1 and Minor version=0 , Flags field is correct and Message ID=0).

References:

RFC2408 : 3.1 ISAKMP Header Format
RFC2409 : 3.1 ISAKMP Header Format

7.1.2 Security Association Payload format

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or Transform(3) payload. Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 0).
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload.
  (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload.
  Implementations MUST support SIT_IDENTITY_ONLY.
  (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- Termination

  Clean up SAD and SPD

Judgment:

The first message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).(cookie is set to Initiator cookie filed,Major version=1 and Minor version=0 , Flags field is correct and Message ID=0).

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing
RFC2409 : 4. Introduction

7.1.3 Proposal Payload format

Purpose:

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In Phase I, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In Phase I, this field contain the value "1".)
- Protocol-ID field
  All implementations within the IPSEC DOI MUST support PROTO_ISAKMP.
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.
  (In Phase I, this field is redundant and MAY be set to 0 or it MAY contain the transmitting entity's cookie.)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 2.4 Identifying Security Associations

4.4.1.1 PROTO_ISAKMP
RFC2408 : 2.5.2 RESERVED Fields
3.5 Proposal Payload
5.3 Generic Payload Header Processing
5.5 Proposal Payload Processing

7.1.4 Transform Payload format

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field only contain the value "0")
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Transform Payload Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.2.1 KEY_IKE
RFC2408 : 2.5.2 RESERVED Fields
          3.6 Transform Payload
          5.3 Generic Payload Header Processing
          5.6 Transform Payload Processing

7.1.5 Transform Payload format (Multiple Transform Payload)

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field only contain the value "3" and "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1" and "2".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))
- If multiple offers are being made for phase 1 exchanges (Main Mode and Aggressive Mode)they MUST take the form of multiple Transform Payloads for a single Proposal Payload in a single SA payload.To put it another way, for phase 1 exchanges there MUST NOT be multiple Proposal Payloads for a single SA payload and there MUST NOT be multiple SA payloads.
- The multiple transforms MUST be presented with monotonically increasing numbers in the initiator's preference order.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Phase-1 sending multiple proposal)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter

    Any attribute is acceptable as proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I								
			Ex mode	**Key Value**	**Trans #**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	1	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
					2	DES	MD5	pre-shared key	1	8 Hour	
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST		3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- Termination

  Clean up SAD and SPD

Judgment:

The first message's Transform Payload Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.2.1 KEY_IKE
RFC2408 : 2.5.2 RESERVED Fields
          3.6 Transform Payload
          4.2 Security Association Establishment
          5.3 Generic Payload Header Processing
          5.6 Transform Payload Processing

7.1.6 Attributes include MD5

Purpose:

IKE implementations MUST support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

So, IKE implementations MUST support MD5.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	MD5	pre-shared key*	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	MD5	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(MD5:1) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction

7.1.7 Attributes include SHA

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

So, IKE implementations SHOULD support SHA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA	pre-shared key*	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)    Direction     Responder(TN)
(1)  HDR; SA          ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(SHA:2) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.8 Attributes include DES

Purpose:

IKE implementations MUST support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

So, IKE implementations MUST support DES.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DES-CBC)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	DES	SHA*	pre-shared key*	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(DES:1) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.9 Attributes include 3DES

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

So, IKE implementations SHOULD support 3DES.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA*	pre-shared key*	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA*	pre-shared key*	2*	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(3DES:5) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.10 Attributes include AES

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- AES-128 in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

So, IKE implementations SHOULD support AES.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CBC)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	AES	SHA*	pre-shared key*	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	AES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(AES-CBC:7) must be included.
And must conform to above Configuration.

References:

RFC3602 : 5. IKE Interactions
          5.1. Phase 1 Identifier

7.1.11 Attributes include PSK

Purpose:

IKE implementations MUST support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

So, IKE implementations MUST support pre-shared keys.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA*	pre-shared key	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(PSK:1) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.12 Attributes include RSA sign

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - RSA signatures. - MODP over group number two.

So, IKE implementations SHOULD support RSA signatures.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES*	SHA*	RSA signatures	2*	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

* Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

* Termination

  Clean up SAD and SPD

Judgment:

The first message Attributes(RSA sign:3) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.13 Attributes include DH1

Purpose:

IKE implementations MUST support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

So, IKE implementations MUST support DH1.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA*	pre-shared key*	1	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                   Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(DH1:1) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction
          6.1 First Oakley Default Group

7.1.14 Attributes include DH2

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

So, IKE implementations SHOULD support DH2.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA*	pre-shared key*	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(DH2:2) must be included.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.1.15 Attributes include DH5

Purpose:

IKE implementations support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number five.

So, IKE implementations support DH5.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA*	pre-shared key*	5	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(DH5:5) must be included.
And must conform to above Configuration.

References:

RFC3526 : 2. 1536-bit MODP Group

7.1.16 Attributes include

Purpose:

IKE implementations support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number fourteen.

So, IKE implementations support DH14.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES*	SHA*	pre-shared key*	14	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-2 addr

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message Attributes(DH14:14) must be included.
And must conform to above Configuration.

References:

RFC3526 : 3. 2048-bit MODP Group

7.1.17 Key Exchange Payload Format (DH1)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH1)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
         <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuraton.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.1.18 Key Exchange Payload Format DH2

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.1.19 Key Exchange Payload Format DH5

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

* Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)    Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA
(3)  HDR; KE; NONCE   ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

* Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.1.20 Key Exchange Payload Format DH14

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

<IDENTITY PROTECTION EXCHANGE>

```
 #   Initiator(NUT)    Direction    Responder(TN)
(1)  HDR; SA           ========>
(2)                    <========       HDR; SA
(3)  HDR; KE; NONCE    ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.1.21 Nonce Payload Format

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA
(3)  HDR; KE; NONCE   ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message's Nonce Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.13 Nonce Payload Processing
RFC2409 : 5. Exchanges

7.1.22 Encryption of ISAKMP payload

Purpose:

When communication is protected, all payloads following the ISAKMP header MUST be encrypted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>                      <---must be encrypted
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be encrypted and received.
And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format
RFC2409 : 3.2 Notation

7.1.23 Identification Payload Format

Purpose:

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, this field is set as 5(ID_IPV6_ADDR).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port ID field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, this value is NUT IPv6 address.)
- During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA              ========>
(2)                       <========        HDR; SA
(3)  HDR; KE; NONCE       ========>
(4)                       <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
                   Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee

liveness and protect against replay attacks.

5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message's Identification Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
5.3 Generic Payload Header Processing
5.8 Identification Payload Processing

7.1.24 HASH Payload Format

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH_I=prf(SKEYID,g^xi|g^xr|CKY-I|CKY-R|SAi_b|IDii_b))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
         <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message's HASH Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.11 Hash Payload Processing

7.1.25 Implementation of Main Mode with pre-shared key

Purpose:

Implementation of Main Mode with pre-shared key check.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
             <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA             ========>
              Judgement (Check *1)
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
              Judgement (Check *2)
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
              Judgement (Check *3)
(6)                      <========      HDR*; IDir; HASH_R
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

* PHASE II

```
                    <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                Judgement (Check *4)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
  Check *1
    Security Association Payload Format must be base on description of RFC,
  Check *2
    Key Exchange and Nonce Payload Format must be base on description of RFC.
  Check *3
    Identification and Hash Payload Format must be base on description of RFC.
In Phase II, the first message must be received.
  Check *4
    NUT must start Phase II negotiation.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction
          5. Exchanges

7.1.26 Signature Payload Format

Purpose:

Signature Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Signature Data field
  Data that results from applying the digital signature function to the ISAKMP message and/or state.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  ✧ Initiator and Responder generate the public key and the secret key
  ✧ Initiator and Responder exchange the certificate of each other.
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I   ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message's Signature Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.12 Signature Payload Processing

7.1.27 Certificate Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Encoding field
  This field indicates the type of certificate or certificate-related information contained in theCertificate Data field.
- Certificate Data field
  Actual encoding of certificate data

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE; CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I   ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

5. Recieve the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I

is the result of the negotiated digital signature algorithm applied to HASH_I. Additionally the initiator send Certificate and Certificate Request Payload

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message's Certificate Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.9 Certificate Payload
5.3 Generic Payload Header Processing
5.9 Certificate Payload Processing

7.1.28 Certificate Request Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Type field
  Contains an encoding of the type of certificate requested
- Certificate Authority field
  Contains an encoding of an acceptable certificate authority for the type of certificate requested.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
            <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE; CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I   ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I

is the result of the negotiated digital signature algorithm applied to HASH_I.
Additionally the initiator send Certificate and Certificate Request Payload

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message's Certificate Request Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.10 Certificate Request Payload
5.3 Generic Payload Header Processing
5.10 Certificate Request Payload Processing

7.1.29 Implementation of Main Mode with RSA signatures

Purpose:

Implementation of Main Mode with RSA signatures check.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA             ========>
               Judgement (Check *1)
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
               Judgement (Check *2)
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I   ========>
               Judgement (Check *3)
(6)                      <========      HDR*; IDir; SIG_R
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

＊ PHASE II

<QUICK MODE>

```
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                 Judgement (Check *4)
```

The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
Check *1
Security Association Payload Format must be base on description of RFC,
Check *2
Key Exchange and Nonce Payload Format must be base on description of RFC.
Check *3
Identification and Signature Payload Format must be base on description of RFC.
In Phase II, the first message must be received.
Check *4
NUT must start Phase II negotiation.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction
5. Exchanges

7.1.30 Processing Invalid ISAKMP Payload Length

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Length field = 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA        ========>
(2)                 <========     HDR; SA  <-----Length field(ISAKMP header)
                                                          : 0 (invalid)
(3-A)HDR; KE; NONCE  ========> X           <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.1 General Message Processing

7.1.31 Processing invalid Responder Cookie field

Purpose:

Verify the Initiator and Responder "cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    In TEST PROCEDURE, Responder Cookie field of the fourth message of IDENTITY PROTECTION EXCHANGE is set to 0(not same as the second message's responder cookie).
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction   Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========    HDR; SA
(3)  HDR; KE; NONCE   ========>
(4)                   <========  HDR;KE;NONCE <-----Cookie field : 0 (invalid
                                                  (not same as the second
                                                    message(2)'s cookie))
(5-A)HDR*; ID; HASH_I  ========> X            <-----Must not transmit
        or
(5-B)HDR; N/D          ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Receive the fifth message from NUT
   In the fifth message (5-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the third message must be exchanged correctly.
The fourth message must not be accepted. And the fifth message(5-A) must not be returned (* or INVALID-COOKIE message(5-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.1.32 Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ISAKMP Header Format(HOST-2:Responder)
    Next Payload field = 127(invalid)
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)    Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========     HDR; SA    <-----Next Payload field
                                                  (ISAKMP Header):127(invalid)
(3-A)HDR; KE; NONCE   ========> X              <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.1.33 Processing invalid Major Version field (major 15, minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:responder)
    Major Version : 15 (invalid value)
    Minor Version : 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)    Direction   Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========      HDR; SA  <-----Major Version : 15(invalid)
(3-A)HDR; KE; NONCE    ========> X             <-----Must not transmit
        or
(3-B)HDR; N/D          ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* orINVALID-MAJOR-VERSION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.1.34 Processing invalid Minor Version field (major 1, minor 15)

Purpose:

Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.

Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Major Version : 1
    Minor Version : 15 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>
(2)                   <========     HDR; SA    <-----Minor Version : 15(invalid)
(3-A)HDR; KE; NONCE   ========> X               <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                Judgement (Check *1)
```

1. Recieve the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-MINOR-VERSION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.1.35 Processing invalid Exchange Type field

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Exchange Type field = 31 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========     HDR; SA   <-----Exchange Type field : 31
                                                                  (invalid)
(3-A)HDR; KE; NONCE  ========> X             <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.1.36 Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate systemaudit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Flags field = |1|1|1|1|1|0|0|0| (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)    Direction   Responder(TN)
(1)  HDR; SA          ========>
(2)                 <========     HDR; SA  <----Flags field : |1|1|1|1|1|0|0|0|
                                                              (invalid value)
(3-A)HDR; KE; NONCE  ========> X          <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-FLAGS message(3-B) is returned).

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.1.37 Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values. If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Message ID field = 1 (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)  Direction   Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========     HDR; SA     <-----Message ID  field : 1
                                                            (invalid value)
(3-A)HDR; KE; NONCE  ========> X               <-----Must not transmit
         or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned(* or INVALID-MESSAGE-ID message(3-B) is returned).

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.1.38 Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    RESERVED field : 1 (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========     HDR; SA     <-----RESERVED field : 1
                                                        (SA, invalid value)
(3-A)HDR; KE; NONCE  ========> X               <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.1.39 Processing invalid Next Payload field

Purpose:

- This field MUST NOT contain the values for the Proposal or Transform payloads as they are considered part of the security association negotiation.
- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    Next Payload field : **2**(Proposal Payload, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA        ========>
(2)                 <========       HDR; SA     <-----Next Payload field(SA) :
                                                              2(invalid value)
(3-A)HDR; KE; NONCE ========> X                 <-----Must not transmit
         or
(3-B)HDR; N/D         ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(3-B) is returned).

References:

RFC2408 : 3.4 Security Association Payload
5.3 Generic Payload Header Processing

7.1.40 Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported.
If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    Domain of Interpretation field : 0xffffffff (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========     HDR; SA      <-----DOI field : 0xffffffff
                                                            (invalid value)
(3-A)HDR; KE; NONCE  ========> X                <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or DOI-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.41 Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    Situation field : 0x80000000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA     <-----Situation field :
                                                    0x80000000(invalid value)
(3-A)HDR; KE; NONCE  ========> X                  <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-B) must not be returned (* or SITUATION-NOT-SUPPORTED message(3-A) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.42 Processing invalid proposal (Encryption Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	65000	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA     <-----Invalid proposal
(3-A)HDR; KE; NONCE  ========> X                 <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned(* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.43 Processing invalid field proposal (Hash Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	65000	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA     <-----Invalid proposal
(3-A)HDR; KE; NONCE  ========> X                 <-----Must not transmit
         or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.44 Processing invalid field proposal (Authentication method)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	65000	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA     <-----Invalid proposal
(3-A)HDR; KE; NONCE  ========> X                 <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.45 Processing invalid field proposal (Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	32767	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA     <-----Invalid proposal
(3-A)HDR; KE; NONCE  ========> X                 <-----Must not transmit
         or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.46 Processing invalid proposal (Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA attribute(HOST-2:Responder, In Phase II)
    Life Type : 65000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA     <-----Invalid proposal
(3-A)HDR; KE; NONCE   ========> X                 <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.1.47 Processing invalid Protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Responder)
    Protocol-ID field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA    <-----Protocol-ID field : 248
                                                               (invalid value)
(3-A)HDR; KE; NONCE  ========> X                <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PROTOCOL-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.1.48 Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Responder)
    SPI field : SPI value is set as 1 (not same as cookie value, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)    Direction     Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========     HDR; SA   <-----SPI field : 1(invalid value)
(3-A)HDR; KE; NONCE   ========> X             <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-SPI message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.1.49 Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Responder)
    Number of Transforms field : 0(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA     <-----Number of Transforms
                                                     field : 0(invalid value)
(3-A)HDR; KE; NONCE  ========> X                 <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:
RFC2408 : 5.5 Proposal Payload Processing

7.1.50 Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - Transform Payload Format(HOST-2:Responder)
    Transform-ID field : 248(invalid value)
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA     <-----Transform-ID field : 248
                                                                (invalid value)
(3-A)HDR; KE; NONCE  ========> X                  <-----Must not transmit
        or
(3-B)HDR; N/D        ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-TRANSFORM-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.1.51 Processing invalid Transform Payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Responder)
    SA Attributes field : not set (see below)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST						SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

In order to start the negotiation of IKE,
TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA     <-----SA Attributes field :
                                                          not set (invalid)
(3-A)HDR; KE; NONCE   ========> X                 <-----Must not transmit
        or
(3-B)HDR; N/D         ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or BAD-PROPOSAL-SYNTAX , PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.1.52 Multiple Transform Payloads(modify proposal)

Purpose:

- If the initiator of an exchange notices that attribute values have changed or attributes have been added or deleted from an offer made, that response MUST be rejected.
- The initiator MUST verify that the Security Association payload received from the responder matches one of the proposals sent initially.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  Any attribute is acceptable as proposal.

  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**								
			Ex mode	**Key Value**	**Trans #**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	1	DES	MD5	pre-shared key	2	8 Hour	SGW-1 addr
					2	3DES	SHA	pre-shared key	2	8 Hour	
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST		65000	65000	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)   Direction    Responder(TN)
(1)  HDR; SA         ========>
(2)                  <========     HDR; SA    <-----modify proposal (invalid)
(3)  HDR; KE; NONCE  ========> X                 <-----Must not transmit
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned.

References:

RFC2408 : 4.2 Security Association Establishment
RFC2409 : 5. Exchanges

7.1.53 Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Key Exchange Payload Format(HOST-2:Responder)
    Key Exchange Data field : 0(1byte) (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)      Direction    Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========     HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <======== HDR; KE; NONCE <-----Key Exchange Data field :
                                                              0(1byte)(invalid)
(5-A)HDR*; IDii; HASH_I ========> X                     <-----Must not transmit
          or
(5-B)HDR; N/D            ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protectionsuite it has accepted with the Security Association, Proposal, andTransform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth message (5-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the third message must be exchanged correctly.
The fourth message must not be accepted. And the fifth message(5-A) must not be

returned (* or INVALID-KEY-INFORMATION message(5-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.7 Key Exchange Payload Processing

7.1.54 Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Identification Payload Format(HOST-2:Responder)
    ID Type field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
(1)  HDR; SA            ========>
(2)                     <========   HDR; SA
(3)  HDR; KE; NONCE     ========>
(4)                     <========   HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>
(6)                     <========  HDR*; IDir; HASH_R <----ID Type field : 248
                                                           (invalid value)
(7)  HDR*; HASH(1); N/D ========>                 <----Must not start Phase II
     (HDR; N/D)
              Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And Phase II must not start (* or INVALID-ID-INFORMATION message(7) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.8 Identification Payload Processing

7.1.55 Not include Identification Payload

Purpose:

All IPSEC DOI implementations MUST support SIT_IDENTITY_ONLY by including an Identification Payload in at least one of the Phase I Oakley exchanges and MUST abort any association setup that does not include an Identification Payload.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Responder(TN) does not send ID payload by the the sixth message.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii;
         HASH_I          ========>
(6)                      <========     HDR*; HASH_R <----not include ID payload
                                                              (invalid)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
   In this test, TN does not send identification information(ID payload).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

＊ PHASE II

```
                      <QUICK MODE>
#   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
           SA, Ni       ========>                 <----must not start Phase II
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And Phase II must not start
(Not establish ISAKMP SA, Not start negotiation of Phase II).

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY

7.1.56 Invalid Identification Payload receive

Purpose:

During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500. If an implementation receives any other values, this MUST be treated as an error and the security association setup MUST be aborted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Responder(TN)'s port fields of ID payload is set to 300. (invalid value)
  - ✧ Responder(TN)'s protocol ID fields of ID payload is set to TCP. (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR; SA            ========>
(2)                     <========         HDR; SA
(3)  HDR; KE; NONCE     ========>
(4)                     <========       HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>
(6)                     <========     HDR*; IDir; HASH_R <----ID protocol/port :
                                                          TCP/300(invalid value)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
          SA, Ni        ========> X                  <----must not start Phase II
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
   And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I the first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And In Phase II the first message must not be returned(Not establish ISAKMP SA, Not start negotiation of Phase II).

References:

RFC2407 : 4.6.2 Identification Payload Content

7.1.57 Processing invalid Hash Payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriatesystem audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Responder)
    Hash Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
(1)HDR; SA          ========>
(2)                 <======== HDR; SA
(3)HDR;KE;NONCE     ========>
(4)                 <======== HDR;KE;NONCE
(5)HDR*;IDii;HASH_I========>
(6)                 <========HDR*;IDir;HASH_R <----Hash Data field : not include
                                                       this field (invalid)
(7)HDR*;HASH(1);N/D========>                 <----Must not start Phase II
   (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).
7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or INVALID-HASH-INFORMATION message is returned.(Not establish ISAKMP SA, Not start negotiation of Phase II).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.1.58 Processing invalid Hash Data field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Hash Payload Format(HOST-2:Responder)
    Hash Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>
(6)                      <======== HDR*; IDir; HASH_R  <----Hash Data field : 0
                                                                  (invalid)
(7)  HDR*;HASH(1);N/D   ========>                <----Must not start Phase II
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or AUTHENTICATION-FAILED message is returned).
(Not establish ISAKMP SA, Not start negotiation of Phase II).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.1.59 Processing invalid Signature Payload

Purpose:

Determine if the Signature is supported. If the Signature determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SIGNATURE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key.
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Responder)
    Signature Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
# Initiator(NUT)  Direction Responder(TN)
(1)  HDR; SA      ========>
(2)               <========  HDR; SA
(3)HDR;KE;NONCE   ========>
(4)               <========HDR; KE; NONCE
(5)HDR*;IDii;SIG_I========>
(6)               <========HDR*;IDir;SIG_R <---Signature Data field:not
                                               include this field(invalid)
(7)HDR*;HASH(1);N/D========>               <----Must not start Phase II
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
6. Send the sixth message from TN

In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fifth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or INVALID-SIGNATURE message is returned.(Not establish ISAKMP SA, Not start negotiation of Phase II).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

7.1.60 Processing invalid Signature Data field

Purpose:

Perform the Signature function as outlined in the DOI and/or Key Exchange protocol documents. If the Signature function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Responder)
    Signature Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)     Direction      Responder(TN)
(1)  HDR; SA            ========>
(2)                     <========       HDR; SA
(3)  HDR; KE; NONCE     ========>
(4)                     <========     HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I  ========>
(6)                     <======== HDR*; IDir; SIG_R  <---Signature Data field :
                                                                     0(invalid)
(7)  HDR*; HASH(1); N/D ========>                  <----Must not start Phase II
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and

the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.
7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or AUTHENTICATION-FAILED message is returned.(Not establish ISAKMP SA, Not start negotiation of Phase II).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

7.1.61 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    Cert Encoding Type fild: 255 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========      HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========HDR; KE; NONCE; CERT Req <---Cert Encoding Type
(5-A)HDR*; IDii; CERT;                                        fild:255(invalid)
      CERT Req; SIG_I ========> X                          <---must not transmit
         or
(5-B)HDR*; HASH(1); N/D ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

5. Receive the fifth message from NUT
   In the fifth message (5-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

The first and the third message must be exchanged correctly.
The fourth message must not be accepted. And the fifth message(5-A) must not be returned (* or INVALID-CERT-ENCODING message(5-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.1.62 Processing invalid Certificate Authority field

Purpose:

Determine if the Certificate Authority is supported for the specified Certificate Encoding. If the Certificate Authority is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE AUTHORITY, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-AUTHORITY message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    Certificate Authority field: 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

* Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <======== HDR;KE;NONCE;CERT Req <---Cert Data field:
(5-A)HDR*; IDii; CERT;                                           0(invalid)
      CERT Req; SIG_I   ========> X                    <---must not transmit
         or
(5-B)HDR*; HASH(1); N/D ========>
     (HDR; N/D)
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

5. Receive the fifth message from NUT
   In the fifth message (5-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the third message must be exchanged correctly.
The fourth message must not be accepted. And the fifth message(5-A) must not be returned (* or INVALID-CERT-ENCODING message(5-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.1.63 Processing invalid Certificate Type with Certificate Authority

Purpose:

Process the Certificate Request. If a requested Certificate Type with the specified Certificate Authority is not available, then the payload is discarded and the following actions are taken:

(a) The event, CERTIFICATE-UNAVAILABLE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the CERTIFICATE-UNAVAILABLE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    Certificate Authority field: Distinguish Name
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #  Initiator(NUT)  Direction   Responder(TN)
(1)  HDR; SA         ========>
(2)                 <========     HDR; SA
(3) HDR;KE;NONCE     ========>
(4)                  <======== HDR;KE;NONCE;CERT Req<---Certificate Data field
                                                     : The value which is
                                                      not available for
(5-A)HDR*;IDii;CERT;                                  Certificate Authority
     CERT Req;SIG_I  ========> X                   <---must not transmit
          or
(5-B)HDR*;HASH(1);N/D========>
    (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

5. Receive the fifth message from NUT
   In the fifth message (5-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the third message must be exchanged correctly.
The fourth message must not be accepted. And the fifth message(5-A) must not be returned (*or CERTIFICATE-UNAVAILABLE message(5-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.1.64 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is not supported, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Responder)
    Cert Encoding field : 255(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(NUT)     Direction      Responder(TN)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE; CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I   ========>
(6)                   <========HDR*; IDir;CERT; SIG_R <---Cert Encoding field :
                                                                255(invalid)
(7)  HDR*; HASH(1); N/D ========>                 <----must not start PhaseⅡ
                  Judgement (Check *1)                              (HDR; N/D)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload

6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R. Additionally the responder send Certificate Request Payload.
7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the fifth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or INVALID-CERT-ENCODING message is returned).
(Not establish ISAKMP SA, Not start negotiation of Phase II).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

7.1.65 Processing invalid Certificate Date field

Purpose:

Process the Certificate Data field. If the Certificate Data is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERTIFICATE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Responder)
    Certificate Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 # Initiator(NUT)  Direction  Responder(TN)
(1)HDR; SA         ========>
(2)               <========    HDR; SA
(3)HDR;KE;NONCE    ========>
(4)               <======== HDR;KE;NONCE;CERT Req
(5)HDR*;IDii;CERT;
   CERT Req; SIG_I ========>
(6)               <======== HDR*;IDir;CERT;SIG_R  <----Certificate Encoding
                                                         field:0(invalid)
(7)HDR*;HASH(1);N/D ========>                    <----must not start Phase II
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Receive the third message from NUT
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Send the fourth message from TN
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

5. Receive the fifth message from NUT
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

Additionally the initiator send Certificate and Certificate Request Payload

6. Send the sixth message from TN
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R. Additionally the responder send invalid Certificate Request Payload.
7. Receive the seventh message from NUT
   In the seventh message (7), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the fifth message must be exchanged correctly.
The sixth message must not be accepted. And the seventh message must not be returned (* or INVALID-CERTIFICATE message is returned).
(Not establish ISAKMP SA, Not start negotiation of Phase II) *option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

7.2.1 Encryption of ISAKMP payload

Purpose:

The information exchanged along with Quick Mode MUST be protected by the ISAKMP SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be encrypted and received.
And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format

7.2.2 Position of payload

Purpose:

In Quick Mode, a HASH payload MUST immediately follow the ISAKMP header and a SA payload MUST immediately follow the HASH.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                    <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has correct position of payload must be received.
And must conform to above Configuration.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.2.3 ISAKMP Header Format (Phase II)

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Initiator cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 8(Hash Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  Indicates the type of exchange being used.
  (In this test, this field is set as 32(Quick mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission.
  |0|0|0|0|0|A|C|E|
- Message ID field
  Unique Message Identifier used to identify protocol state during Phase 2 negotiations.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                      <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 3.1 ISAKMP Header Format
5.2 ISAKMP Header Processing
RFC2409 : 4. Introduction

7.2.4 HASH Payload Format

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.

- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.

- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH(1)=prf(SKEYID_a,M-ID|SA|Ni[|KE][|IDci|IDcr))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                    <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's HASH Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.11 Hash Payload Processing

7.2.5 Security Association Payload format check(Phase II)

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or Transform(3) payload.
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload.
  (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload.
  Implementations MUST support SIT_IDENTITY_ONLY.
  (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
In Phase II, the first message's Security Association Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY
RFC2408 : 2.5.2 RESERVED Fields
3.4 Security Association Payload
5.3 Generic Payload Header Processing
5.4 Security Association Payload Processing

7.2.6 Proposal Payload format (Phase II)

Purpose:

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0"
  (In this test, value is 0).
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In this test, this field contain the value "1".)
- Protocol-ID field
  Specifies the protocol identifier for the current negotiation.
  (In this test, this field contain the value "3"(PROTO_IPSEC_ESP))
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                         <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 2.5.2 RESERVED Fields
3.5 Proposal Payload
5.3 Generic Payload Header Processing
5.5 Proposal Payload Processing

7.2.7 Transform Payload Format (Phase II)

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0"
  (In this test, value is 3 and 0).
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In this test, this field contain "3"(ESP_3DES),"2"(ESP_DES))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans #	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	1	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
				2	ESP_DES	Tunnel	HMAC-SHA	8 Hour			
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP		ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.

In Phase II , the first message's Transform Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 2.5.2 RESERVED Fields
3.6 Transform Payload
5.3 Generic Payload Header Processing
5.6 Transform Payload Processing

7.2.8 Transform Payload Format (Multiple Transform) (Phase II)

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0"
  (In this test, value is 3 and 0).
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
- The multiple transforms MUST be presented with monotonically increasing numbers in the initiator's preference order.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Phase-2 sending multiple proposal)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal in Phase I.
    Any attribute is acceptable in Phase II.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans #**	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	1	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
				2	ESP_DES	Tunnel	HMAC-SHA	8 Hour			
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP		ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Transform Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 2.5.2 RESERVED Fields
3.6 Transform Payload
5.3 Generic Payload Header Processing
5.6 Transform Payload Processing

7.2.9 Transform payload SA Attributes(ESP_DES,HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DES-CBC, HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

＊ PHASE Ⅰ
For Phase-1 Sequence, refer ″4.1Phase-1 Sequence (Initiator Test)″

Procedure:

The test sequence is following.

＊ PHASE Ⅱ

```
                        <QUICK MODE>
 #    Initiator(NUT)       Direction        Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase Ⅰ, messages must be exchanged correctly.
In Phase Ⅱ, the first message which has ESP_DES and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.2 ESP_DES
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.10 Transform payload SA Attributes (ESP_3DES, HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI are strongly encouraged to support ESP_3DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3. (see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                       <QUICK MODE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_3DES and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.3 ESP_3DES
          4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.11 Transform payload SA Attributes (ESP_3DES,HMAC-SHA)

Purpose:

- All implementations within the IPSEC DOI are strongly encouraged to support ESP_3DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

＊PHASE Ⅰ

For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

＊PHASE Ⅱ

```
                        <QUICK MODE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase Ⅰ, messages must be exchanged correctly.
In Phase Ⅱ, the first message which has ESP_3DES and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.3 ESP_3DES
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.12 Transform payload SA Attributes(ESP_3DES,AES-XCBC-MAC)

Purpose:

- AES-128 in CBC mode for HMAC function SHOULD be supported
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support AES-XCBC-MAC)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	AES-XCBC-MAC	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	AES-XCBC-MAC	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I

For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                       <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_3DES and Auth(AES-XCBC-MAC) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC3566 : 6. IANA Considerations
RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.13 Transform payload SA Attributes (ESP_AES(128bit),HMAC-SHA)

Purpose:

- AES-128 in CBC mode [RFC3602] SHOULD be supported
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CBC (128bit))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_AES and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC3602 : 5. IKE Interactions
5.2.Phase 2 Identifier
RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.14 Transform payload SA Attributes (ESP_NULL,HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL, HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

In order to start the negotiation of IKE,
TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                    <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_NULL and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.11 ESP_NULL
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.15 Transform payload SA Attributes (ESP_NULL,HMAC-SHA)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3. (see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

In order to start the negotiation of IKE,
TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
              Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_NULL and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.11 ESP_NULL
          4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.16 Transform payload SA Attributes (ESP_NULL,AES-XCBC-MAC)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL, AES-XCBC-MAC)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	AES-XCBC-MAC	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	AES-XCBC-MAC	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

In order to start the negotiation of IKE,
TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has ESP_NULL and Auth(AES-XCBC-MAC) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.11 ESP_NULL
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.17 ESP without Authentication Algorithm(ESP_DES)

Purpose:

When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication), DES-CBC)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-1:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points). And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attributes

7.2.18 ESP without Authentication Algorithm(ESP_3DES)

Purpose:

When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Transform Payload Format(HOST-1:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                      <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points). And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attributes

7.2.19 ESP without Authentication Algorithm(ESP_AES)

Purpose:

- When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication), AES-CBC (128bit))

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Transform Payload Format(HOST-1:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel		8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel		8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attributes
          4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.2.20 enable PFS with DH1

Purpose:

- DH Group
  Oakley implementations MUST support a MODP group with the following prime and generator. This group is assigned id 1 (one).
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode. While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                      <QUICK MODE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1), SA,
    Ni, KE, IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has KE payload and DH1 as SA attribute must be received.
And must conform to above Configuration.

References:

RFC2409 : 3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
6.1 First Oakley Default Group

7.2.21 enable PFS with DH2

Purpose:

- DH Group
  IKE implementations SHOULD support a MODP group with the following prime and generator. This group is assigned id 2 (two).
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys,and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode. While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <QUICK MODE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                   Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has KE payload and DH2 as SA attribute must be received.
And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
6.2 Second Oakley Group

7.2.22 enable PFS with DH5

Purpose:

- DH Group
  IKE implementations support a 1536 bit MODP group.
  This group is assigned id 5.
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys,and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode.While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH5)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                         <QUICK MODE>
 #   Initiator(NUT)       Direction       Responder(TN)
(1)  HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                   Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has KE payload and DH5 as SA attribute must be received.
And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
          5.5 Phase 2 - Quick Mode
RFC3526 : 2. 1536-bit MODP Group

7.2.23 enable PFS with DH14

Purpose:

- DH Group
  IKE implementations support a 2048 bit MODP group.
  This group is assigned id 14.
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode. While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(NUT)       Direction        Responder(TN)
(1)  HDR*, HASH(1), SA,
    Ni, KE, IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which has KE payload and DH14 as SA attribute must be received.
And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
          5.5 Phase 2 - Quick Mode
RFC3526 : 3. 2048-bit MODP Group

7.2.24 consistent of proposal (Diffie-Hellman Group(Transform Payload))

Purpose:

All offers made during a Quick Mode are logically related and must be consistant. For example, if a KE payload is sent, the attribute describing the Diffie-Hellman group (see section 6.1 and [Pip97]) MUST be included in every transform of every proposal of every SA being negotiated.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Phase-2 sending multiple proposal)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    Any attribute is acceptable as proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II									
			Proto ID	Trans #	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	1	ESP_DES	Tunnel	HMAC-MD5	2	8 Hour	Net-z addr	Net-v addr	any
				2	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour			
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP		ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                      <QUICK MODE>
#   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Diffie-Hellman Group of multiple offers must be same.
And must conform to above Configuration.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.2.25 Key Exchange Payload Format(DH1) (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH1)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                       <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1), SA,
    Ni, KE, IDci, IDcr; ========>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.2.26 Key Exchange Payload Format(DH2) (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 #    Initiator(NUT)       Direction        Responder(TN)
(1)  HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.2.27 Key Exchange Payload Format (DH5) (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(NUT)       Direction       Responder(TN)
(1)   HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.2.28 Key Exchange Payload Format (DH14) (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

In order to start the negotiation of IKE,
TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <QUICK MODE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination

Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.In Phase II , the first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.2.29 Nonce Payload Format (Phase II)

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message's Nonce Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.13 Nonce Payload Processing
RFC2408 : 5. Exchanges

7.2.30 Key Exchange Payload w/o PFS

Purpose:

If PFS is not needed, and KE payloads are not exchanged

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
 #    Initiator(NUT)       Direction        Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                        <--- must not send KE
payload.
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which must not has KE payload,must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.2.31 Identification Payload Format (Phase II,Tunnel mode to SGW)

Purpose:

ID Payload Format(See below Configuration of Identification Payload Format.)

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.
  (In this test, IDci's this field is set as 6(ID_IPV6_ADDR_SUBNET).
  IDcr's this field is set as 6(ID_IPV6_ADDR_SUBNET).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, IDci's this field has
  3ffe:501:ffff:100::,ffff:ffff:ffff:ffff ::(Net-z network address).
  IDcr's this field has 3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::(Net-v network address).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(D_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field :
    3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::
  - ✧ Identification Payload Format(IDcr, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field :
    3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; =======>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message which Identification Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
        : 5.3 Generic Payload Header Processing
          5.8 Identification Payload Processing
RFC2409 : 5.5 Phase 2 - Quick Mode

7.2.32 Identification Payload Format (Phase II,Tunnel mode to HOST)

Purpose:

ID Payload Format(See below Configuration of Identification Payload Format.)

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, IDci's this field is set as 6(ID_IPV6_ADDR_SUBNET).
  IDcr's this field is set as 5(ID_IPV6_ADDR).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, IDci's this field has
  3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::(Net-z network address).
  IDcr's this field has 3ffe:501:ffff:103::11(TN(HOST-2) IPv6 address).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 2 Topology for SGW vs. HOST (Initiator Test)".
- **Configuration**
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(D_IPV6_ADDR_SUBNET)

Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field
: 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::

✧ Identification Payload Format(IDcr, In Phase II)
Identification Type field : 5(ID_IPV6_ADDR)
Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field : 3ffe:501:ffff:103::11

✧ Initiator and Responder IKE parameter
At least, following parameter must be included in proposal.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	HOST-2 addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	HOST-2 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                     <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; =======>
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association,

Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
In Phase II, the first message which Identification Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
3.8 Identification Payload

7.2.33 HASH Payload Format check(Phase II)

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH(3) = prf(SKEYID_a, 0 | M-ID | Ni_b | Nr_b))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)       ========>
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

- **Termination**

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second message must be exchange correctly.
The third message's HASH Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.11 Hash Payload Processing

7.2.34 set Commit Bit(CONNECTED Notify Message)

Purpose:

If set(1), the entity which did not set the Commit Bit MUST wait for an Informational Exchange containing a Notify payload (with the CONNECTED Notify Message) from the entity which set the Commit Bit.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Commit bit)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Responder(TN)'s Commit Bit of ISAKMP header is set to 1 in Phase II.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========   HDR*, HASH(2), SA, Nr  <--- Commit Bit = 1
                                      IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
(4)                     <========   HDR*; HASH(1), N/D     <--- Commit Bit = 1
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.
4. Send the fourth message from TN
   In the fourth message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload. In this case, the initiator send CONNECTED Notify Message.

* IPsec transmission

```
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>              <--- Must not send before recive
              Judgement (Check *1)                 the CONNECTED Notify Message.
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
And must NUT wait for an Informational Exchange containing a Notify payload(with the CONNECTED Notify Message).
NUT must not forward Echo Request before recive the CONNECTED Notify Message.
After NUT revive the CONNECTED Notify Message, NUT must forward Echo Request with IPsec SA.
And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format

7.2.35 Implementation of Quick Mode(ESP_3DES (Tunnel mode to SGW))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#    Initiator(NUT)      Direction      Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                 Judgement (Check *1)
(2)                        <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)       ========>
                 Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #    Initiator(NUT)      Direction      Responder(TN)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>
                 Judgement (Check *3)
```

1. Receive the first message from NUT

In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1
    Hash, Security Association, Nonce, Identification Payload Format must be base on description of RFC.
  Check *2
    Hash Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be received.
  Check *3
    NUT must forward Echo request to SGW-2 with IPsecSA.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.2.36 Implementation of Quick Mode (ESP_3DES and HMAC-SHA(Tunnel mode to SGW))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                      <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
                Judgement (Check *1)
(2)                        <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)        ========>
                Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #    Initiator(NUT)      Direction       Responder(TN)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>
                Judgement (Check *3)
```

1. Receive the first message from NUT
In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN)

to responder (TN) with IPsec SA.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1
    Hash, Security Association, Nonce, Identification Payload Format must be base on description of RFC.
  Check *2
    Hash Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be received.
  Check *3
    NUT must forward Echo request to SGW-2 with IPsecSA.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.2.37 Implementation of Quick Mode (ESP_3DES(Tunnel mode to HOST))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- Network Topology
  Refer the topology "Figure 2 Topology for SGW vs. HOST (Initiator Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	HOST-2 addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-z addr	HOST-2 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                     <QUICK MODE>
 #   Initiator(NUT)     Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
(2)                     <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
               Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #   Initiator(NUT)     Direction      Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
               Judgement (Check *3)
```

1. Receive the first message from NUT

In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1
    Hash, Security Association, Nonce, Identification Payload Format must be base on description of RFC.
  Check *2
    Hash Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be received.
  Check *3
    NUT must forward Echo request to HOST-2 with IPsecSA.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.2.38 Implementation of Quick Mode (ESP_3DES and HMAC-SHA(Tunnel mode to HOST))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 2 Topology for SGW vs. HOST (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	HOST-2 addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	HOST-2 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

＊ PHASE II

```
                         <QUICK MODE>
#   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
               Judgement (Check *1)
(2)                      <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)       ========>
               Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ IPsec transmission

```
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
               Judgement (Check *3)
```

1. Receive the first message from NUT

In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
Check *1
Hash, Security Association, Nonce, Identification Payload Format must be base on description of RFC.
Check *2
Hash Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be received.
Check *3
NUT must forward Echo request to HOST-2 with IPsecSA.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.2.39 Implementation of Quick Mode with PFS

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr; ========>
                Judgement (Check *1)

(2)                      <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
(3)  HDR*, HASH(3)       ========>
                Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

* IPsec transmission

```
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
                Judgement (Check *3)
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder(TN) with IPsec SA.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1
    Hash, Security Association, Nonce, Key Exchange, Identification Payload Format must be base on description of RFC.
  Check *2
    Hash Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be received.
  Check *3
    NUT must forward Echo request to SGW-2 with IPsecSA.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.2.40 Re-keying of IPsec SA

Purpose:

When the SA expires, all keys negotiated under the association (AH or ESP) must be renegotiated.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <the first QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)       ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

* the first IPsec transmission

```
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>
                   Judgement #1 (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with 1st IPsec SA.

In order to start the negotiation of the second Phase II(re-keing), TN(HOST-1) transmits Echo Request to TN(HOST-2) every 3 seconds.

* PHASE II

```
                     <the second QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

* the second IPsec transmission

```
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)   ========>
                 Judgement #2 (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with 1st or 2nd IPsec SA.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second IPsec SA must be established correctly.
In the second IPsec SA transmission, the first message using the first or the second IPsec SA must be received.
And must conform to above Configuration.

References:

RFC2408 : 4.3 Security Association Modification

7.2.41 Using new SA for outbound traffic

Purpose:

A protocol implementation SHOULD begin using the newly created SA for outbound traffic and SHOULD continue to support incoming traffic on the old SA until it is deleted or until traffic is received under the protection of the newly created SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	30 sec	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	30 sec	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

＊PHASE II

<the first QUICK MODE>

#	Initiator(NUT)	Direction	Responder(TN)
(1)	HDR*, HASH(1), SA, Ni, IDci, IDcr;	========>	
(2)		<========	HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)	HDR*, HASH(3)	========>	

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊the first IPsec transmission

#	Initiator(NUT)	Direction	Responder(TN)
(1)	IP_HDR; ESP*; ICMP(Echo request)	========>	
		Judgement (Check *1)	

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

In order to start the negotiation of the second Phase II(re-keing),
TN(HOST-1) transmits Echo Request to TN(HOST-2) every 3 seconds.

```
 * PHASE II
                       <the second QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * the second IPsec transmission

 #   Initiator(NUT)      Direction       Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)   ========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN)

to responder(TN) using IPsec SA that established by the second QUICK MODE.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second IPsec SA must be established correctly.
In the second IPsec SA transmission, the first message using the second IPsec SA must be received.
And must conform to above Configuration.

References:

RFC2408 : 4.3 Security Association Modification

7.2.42 Using both old and new SA for incoming traffic

Purpose:

A protocol implementation SHOULD begin using the newly created SA for outbound traffic and SHOULD continue to support incoming traffic on the old SA until it is deleted or until traffic is received under the protection of the newly created SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	30 sec	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	30 sec	Net-z addr	Net-v addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <the first QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * the first IPsec transmission

 #   Initiator(NUT)      Direction       Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
                 Judgement #1
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder (TN) with IPsec SA.

In order to start the negotiation of the second Phase II(re-keing), TN(HOST-1) transmits Echo Request to TN(HOST-2) every 3 seconds.

```
 * PHASE II
                       <the second QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ the second IPsec transmission

```
# Host(TN)     Initiator(NUT)    Direction    Responder(TN)
(1)       =======>ICMP
                   (Echo request)
(2)                               =======> IP_HDR; ESP*; ICMP(Echo requesst)
                                 Judgement #2
(3)                               <====== IP_HDR; ESP*; ICMP <---This message is
                                             (Echo requesst)       sent before the
(4)     <=======ICMP(Echo request)                                  1st SA expires.
      Judgement #3
(5)                                <====== IP_HDR; ESP*; ICMP<----This message is
                                            (Echo requesst)        sent before the
(6)     <=======ICMP(Echo request)                                  2nd SA expires.
      Judgement #4
```

1. Send the 1st message from NUT
   HOST-1(TN) send Echo request to HOST-2(TN)
2. Receive the 1st message from NUT
   Initiator(NUT) encapuslate it using IPsec SA that established by 2nd QUICK MODE and forward it to Responder(TN).
3. Send the 1st message from TN
   Responder(TN) send ecapuslated Echo request from HOST-2(TN) to initiator(NUT) using IPsec SA that established by 1st QUICK MODE.
4. Receive the 2nd message from NUT
   Initiator(NUT) decapsulate it using IPsec SA that established by 1st QUICK MODE and forward Echo request from HOST-2(TN) to HOST-1(TN).
5. Send the 3rd message from TN
   Responder(TN) send ecapuslated Echo request from HOST-2(TN) to initiator(NUT) using IPsec SA that established by 2nd QUICK MODE.
6. Receive the 4th message from NUT
   Initiator(NUT) decapsulate it using IPsec SA that established by 2nd QUICK MODE and forward Echo request from HOST-2(TN) to HOST-1(TN).

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second IPsec SA must be established correctly.
1st IPsec trasmission is sent correctly.

And the following condition must be satisfied.
1) The 1st message must be accepted.
2) And 2nd message is fowarded using 2nd IPsec SA.
3) The 3rd message using the 1st IPsec SA must be accepted.
4) And 4th message is fowarded
5) The 5th message using the 2nd IPsec SA must be accepted.
6) And 6th message is fowarded
And must conform to above Configuration.

References:

RFC2408 : 4.3 Security Association Modification

7.2.43 Increasing Sequence Number

Purpose:

Encapsulating Security Payload Packet Format

- Sequence Number
  This unsigned 32-bit field contains a monotonically increasing counter value (sequence number). It is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. Processing of the Sequence Number field is at the discretion of the receiver, i.e., the sender MUST always transmit this field, but the receiver need not act upon it.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-1 addr	HOST-2 addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-1 addr	HOST-2 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

The test sequence is following.

```
 * IPsec transmission

 #    Initiator(NUT)      Direction       Responder(TN)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)   ========>
(2)  IP_HDR; ESP*;
     ICMP(Echo request)   ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to responder(TN) with IPsec SA.
2. Receive the second message from NUT
   In the second message (2), initiator(NUT) forward Echo request from HOST-1(TN) to responder(TN) with IPsec SA.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly,
In IPsec SA transmission, the first message's Sequence Number must be "1".
and the second message's Sequence Number must be "2".
And must conform to above Configuration.

References:

RFC2406 : 2. Encapsulating Security Payload Packet Format
          2.2 Sequence Number
          3.3.3 Sequence Number Generation

7.2.44 Sequence Number Verification

Purpose:

Encapsulating Security Protocol Processing(Inbound Packet Processing)

- Sequence Number
  If the receiver has enabled the anti-replay service for this SA, the receive packet counter for the SA MUST be initialized to zero when the SA is established. For each received packet, the receiver MUST verify that the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packets received during the life of this SA. This SHOULD be the first ESP check applied to a packet after it has been matched to an SA, to speed rejection of duplicate packets.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Receiver)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-1 addr	HOST-2 addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-1 addr	HOST-2 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

＊ PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

＊ PHASE II

```
                         <QUICK MODE>
#    Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)       ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

The test sequence is following.

* IPsec transmission

```
 #   Initiator(NUT)      Direction     Responder(TN)
(1)    IP_HDR; ESP*;
     ICMP(Echo request) ========>
(2)                                IP_HDR; ESP*;
                      <========    ICMP(Echo reply) <------Sequence Number:1
(3)    IP_HDR; ESP*;
     ICMP(Echo request) ========>
(4)                                IP_HDR; ESP*;
                      <========    ICMP(Echo reply) <------Sequence Number:1
                                                                  (invalid)
                                                    <------Must not forward
                 Judgement (Check *1)                         to HOST-1 (TN)
```

1. Receive the first message from NUT.
   At the first message (1), initiator(NUT) forward Echo request from HOST-1(TN) to HOST-2(TN) via responder(TN).
2. Send the 2nd message from TN.
   At the 2nd message (2), responder(NUT) forward Echo reply (Sequence Number:1) from HOST-2(TN) to HOST-1(TN) via initiator(NUT).
3. Receive the third message from NUT.
   In the third message (3), initiator(NUT) forward Echo reply from HOST-1(TN) to HOST-2(TN) via responder(TN).
4. Send the 4th message from TN
   In the third message (4), responder(TN) forward Echo request (Sequence Number:1(invalid)) from HOST-2(TN) to HOST-1(TN) via initiator(NUT).

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly,
In IPsec SA transmission, the 4th message must not be accepted.
And must not be fowarded to HOST-1(TN).

References:

RFC2406 : 3.4.3 Sequence Number Verification

7.2.45 Processing invalid ISAKMP Payload Length

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Length field = 0(invalid value)

  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
# Initiator(NUT)     Direction  Responder(TN)
(1)HDR*,HASH(1),
   SA,Ni,IDci,IDcr;   ========>
(2)                  <========HDR*,HASH(2),SA,Nr<-----Length field
                                IDci, IDcr;       (ISAKMP header):0(invalid)
(3-A)HDR*, HASH(3)    ========> X                 <-----Must not transmit
         or
(3-B)HDR*,HASH(1),N/D========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted.
And the third message(3-A) must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.1 General Message Processing

7.2.46 Processing invalid Responder Cookie field

Purpose:

Verify the Initiator and Responder"cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Responder Cookie field : 0 (not same Responder cookie in Phase I)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)     Direction     Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <======== HDR*,HASH(2),SA,Nr <-----Responder Cookie
                                    IDci, IDcr;          field : 0(invalid)
(3-A)HDR*, HASH(3)      ========> X                  <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                         Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted.
And the third message(3-A) must not be returned (* or INVALID-COOKIE message (3-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.2.47 Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Next Payload field = 127(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

＊ PHASE I

For Phase-1 Sequence, refer ″4.1Phase-1 Sequence (Initiator Test)″

Procedure:

The test sequence is following.

```
 ＊ PHASE II
                         <QUICK MODE>
 #   Initiator(NUT)      Direction     Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <======== HDR*,HASH(2),SA,Nr <-----Next Payload field
                                   IDci, IDcr;        (ISAKMP Header) : 127
                                                                  (invalid)
(3-A)HDR*, HASH(3)      ========> X                 <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send ASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, ut excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned(*or INVALID-PAYLOAD-TYPE message(3-A) is returned).
*option:if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.2.48 Processing invalid Major Version field (major 15,minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:
  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.
  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Major Version 15 (invalid value)
    Minor Version 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 # Initiator(NUT)    Direction   Responder(TN)
(1) HDR*, HASH(1),
   SA,Ni,IDci,IDcr; ========>
(2)                 <=======HDR*,HASH(2),SA,Nr<----Major Version:15(invalid)
                               IDci, IDcr;
(3-A)HDR*, HASH(3)  ========> X              <-----Must not transmit
         or
(3-B)HDR*,HASH(1),N/D========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it

has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted.
And the third message(3-A) must not be returned (* or INVALID-MAJOR-VERSION message(3-B) is returned.
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.2.49 Processing invalid Minor Version field (major 1,minor 15)

Purpose:

- Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Major Version 1
    Minor Version 15(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 #    Initiator(NUT)      Direction     Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========  HDR*, HASH(2), SA, Nr <----Miner Version : 15
                                     IDci, IDcr;                       (invalid)
(3-A)HDR*, HASH(3)        ========> X                   <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it

has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted.
And the third message(3-A) must not be returned (* or INVALID-MINOR-VERSION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.2.50 Processing Exchange Type invalid

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Exchange Type field = 31(invalid value)

  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
 #   Initiator(NUT)      Direction   Responder(TN)
(1) HDR*, HASH(1),
    SA, Ni,IDci, IDcr; ========>
(2)                    <========HDR*, HASH(2), SA, Nr<-----Exchange Type
                                 IDci, IDcr;             field :31 (invalid)
(3-A)HDR*, HASH(3)    ========> X                  <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D========>
                         Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.2.51 Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Flags field = |1|1|1|1|1|0|0|1| (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)     Direction     Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========  HDR*,HASH(2),SA,Nr <-----Flags field :
                                      IDci,IDcr;           |1|1|1|1|1|0|0|1|
                                                                   (invalid)
(3-A)HDR*, HASH(3)        ========> X                    <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-FLAGS message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.2.52 Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values.
If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ISAKMP Header Format(HOST-2:Responder, In Phase II)
    Message ID : 0 (not same as Initiater's Massage ID)
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(NUT)       Direction        Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========    HDR*, HASH(2), SA, Nr <-----Message ID : 0
                                        IDci, IDcr;                    (invalid)
(3-A)HDR*, HASH(3)        ========> X                   <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-MESSAGE-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.2.53 Processing invalid Next Payload field

Purpose:

If the Next Payload field validation fails, the message is discarded.

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ SA Payload Format(HOST-2:Responder, In Phase II)
    Next Payload field : 127(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*, HASH(2), SA, Nr<-----Next Payload field:
                                 IDci, IDcr;                  127(invalid)
(3-A)HDR*, HASH(3)      ========> X               <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                         Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.
   In this test, INVALID-PAYLOAD-TYPE Notify message is send.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be received (* or INVALID-PAYLOAD-TYPE message(3-B) is received).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
5.3 Generic Payload Header Processing

7.2.54 Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder, In Phase II)
    RESERVED field : 1(set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                    <QUICK MODE>
 #   Initiator(NUT)    Direction    Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                    <======== HDR*,HASH(2),SA,Nr <-----RESERVED field: 1
                                 IDci, Idcr;                        (invalid)
(3-A)HDR*, HASH(3)     ========> X                  <-----Must not transmit
       or
(3-B)HDR*, HASH(1), N/D ========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned(* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.2.55 Processing invalid Hash Payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Responder, In Phase II)
    Hash Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                       <QUICK MODE>
 #   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========  HDR*, HASH(2), SA, Nr <-----Hash Data field :
                                    IDci, IDcr;              not include this
                                                               field(invalid)
(3-A)HDR*, HASH(3)        ========> X                      <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-HASH-INFORMATION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.2.56 Processing invalid Hash Date Field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Hash Payload Format(HOST-2:Responder, In Phase II)
    Hash Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #    Initiator(NUT)      Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========  HDR*, HASH(2), SA, Nr <-----Hash Data field :
                                    IDci, IDcr;                      0(invalid)
(3-A)HDR*, HASH(3)       ========> X                     <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or AUTHENTICATION-FAILED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.2.57 Processing invalid Next Payload field

Purpose:

- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:
  (a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.
  (b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - SA Payload Format(HOST-2:Responder, In Phase II)
    Next Payload field : 2(Proposal Payload, invalid value)
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <======== HDR*,HASH(2), SA, Nr<-----Next Payload field :
                                    IDci, IDcr;                      2(invalid)
(3-A)HDR*, HASH(3)       ========> X                    <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                           Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.
   In this test, INVALID-PAYLOAD-TYPE Notify message is send.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be received (* or INVALID-PAYLOAD-TYPE message(3-B) is received).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
          5.3 Generic Payload Header Processing

7.2.58 Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported. If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ SA Payload Format(HOST-2:Responder, In Phase II)
    Domain of Interpretation field : 0xffffffff(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
 #    Initiator(NUT)       Direction       Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========HDR*,HASH(2),SA, Nr<-----DOI field :
                                    IDci, IDcr;           0xffffffff(invalid)
(3-A)HDR*, HASH(3)         ========> X                    <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                           Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or DOI-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.59 Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder, In Phase II)
    Situation field : 0x80000000(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I

For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <QUICK MODE>
 #    Initiator(NUT)     Direction    Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========  HDR*,HASH(2),SA,Nr  <-----Situation field :
                                       IDci, IDcr;                  0x80000000
(3-A)HDR*, HASH(3)        ========> X                    <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or SITUATION-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.60 Processing invalid proposal(ESP Authentication)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	61439	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

＊ PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

＊ PHASE II

```
                        <QUICK MODE>
#   Initiator(NUT)    Direction    Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; =======>
(2)                      <========  HDR*, HASH(2), SA, Nr <-----invalid proposal
                                         IDci, IDcr;
(3-A)HDR*, HASH(3)        ========> X                      <-----Must not transmit
          or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.61 Processing invalid proposal(Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	32767	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I

For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),  SA,
   Ni, KE, IDci, IDcr; ========>
(2)                     <======== HDR*,HASH(2),SA, Nr,KE<-----invalid proposal
                                        IDci, IDcr;
(3-A)HDR*, HASH(3)       ========> X                    <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
In Phase II, the second message must not be accepted. And the third message(3-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(3-B) is returned).

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.62 Processing invalid proposal(Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ SA attribute(HOST-2:Responder, In Phase II)
    Life Type : 65000(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
#    Initiator(NUT)       Direction        Responder(TN)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                        <========  HDR*, HASH(2), SA, Nr <-----invalid proposal
                                            IDci, IDcr;
(3-A)HDR*, HASH(3)         ========> X                      <-----Must not transmit
           or
(3-B)HDR*, HASH(1), N/D ========>
                           Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.63 Processing invalid proposal (Encapsulation Mode)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	61439	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========  HDR*, HASH(2), SA, Nr <-----invalid proposal
                                         IDci, IDcr;
(3-A)HDR*, HASH(3)        ========> X                      <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.2.64 Processing invalid Protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Responder, In Phase II)
    Protocol-ID field : 248(invalid value)]
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	248	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  In order to start the negotiation of IKE,

TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
#   Initiator(NUT)      Direction      Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*,HASH(2),SA,Nr <-----Protocol-ID field :
                                  IDci, IDcr;                   248 (invalid)
(3-A)HDR*, HASH(3)      ========> X                <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PROTOCOL-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.2.65 Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Responder, In Phase II)
    SPI field : SPI value is set as 0.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I

For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <======== HDR*, HASH(2), SA, Nr <-----SPI field : 0
                                  IDci, IDcr;                    (invalid)
(3-A)HDR*, HASH(3)      ========> X                     <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-SPI message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.2.66 Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Responder, In Phase II)
    Number of Transforms field : 0

  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*,HASH(2),SA,Nr<-----Number of Transforms
                                  IDci, IDcr;             field : 0(invalid)
(3-A)HDR*, HASH(3)      ========> X              <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                          Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.2.67 Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Responder, In Phase II)
    Transform-ID field : 248(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	248	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*,HASH(2),SA,Nr <-----Transform-ID field :
                                  IDci, IDcr;                         248(invalid)
(3-A)HDR*, HASH(3)       ========> X                <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                         Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the first message(3-A) must not be returned (* or INVALID-TRANSFORM-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.2.68 Processing invalid Transform Payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Responder, In Phase II)
    SA Attributes field : not set(see below)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP					Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*,HASH(2),SA,Nr<-----invalid SA Attributes
                                    IDci, IDcr;
(3-A)HDR*, HASH(3)       ========> X               <-----Must not transmit
        or
(3-B)HDR*, HASH(1), N/D ========>
                         Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.2.69 Multiple Transform Payloads check(modify proposal)

Purpose:

- If the initiator of an exchange notices that attribute values have changed or attributes have been added or deleted from an offer made, that response MUST be rejected.
- The initiator MUST verify that the Security Association payload received from the responder matches one of the proposals sent initially.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans #	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	1	ESP_DES	Tunnel	HMAC-MD5	8 Hour	Net-z addr	Net-v addr	any
				2	ESP_3DES	Tunnel	HMAC-SHA	8 Hour			
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP		ESP_NULL	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
#   Initiator(NUT)    Direction     Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========  HDR*, HASH(2), SA, Nr <-----modify attribute
                                       IDci, IDcr;
(3-A)HDR*, HASH(3)      ========> X                   <-----Must not transmit
                           Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Send the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Receive the third message from NUT
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted.

And the third message(3-A) must not be received.

References:

RFC2408 : 4.2 Security Association Establishment
RFC2409 : 5. Exchanges

7.2.70 Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Key Exchange Payload Format(HOST-2:Responder, In Phase II)
    Key Exchange Data field : 0(invalid valud)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

* PHASE I
For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
#   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1), SA,
    Ni, KE, IDci, IDcr; ========>
(2)                      <========HDR*,HASH(2),SA,Nr,KE <-----Key Exchange Data
                                 IDci, IDcr;            field:0(1byte)(invalid)
(3-A)HDR*, HASH(3)       ========> X                    <-----Must not transmit
          or
(3-B)HDR*, HASH(1), N/D ========>
                           Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-KEY-INFORMATION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.7 Key Exchange Payload Processing

7.2.71 Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- **Configuration**
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::
  - ✧ Identification Payload Format(IDcr, In Phase II)
    (NUT:SGW-1) Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    (TN:SGW-2) Identification Type field : 248(invalid value)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                       <QUICK MODE>
 #   Initiator(NUT)     Direction    Responder(TN)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========HDR*,HASH(2),SA,Nr,
                                   IDci, IDcr;<----ID Type field : 248(invalid)
(3-A)HDR*, HASH(3)      ========> X          <-----Must not transmit
         or
(3-B)HDR*, HASH(1), N/D ========>
                        Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it

has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. And the third message (3-A) must not be returned (* or INVALID-ID-INFORMATION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.8 Identification Payload Processing

7.2.72 invalid Identification Payload

Purpose:

If the client identities are not acceptable to the Quick Mode responder (due to policy or other reasons), a Notify payload with Notify Message Type INVALID-ID-INFORMATION (18) SHOULD be sent.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for SGW vs. SGW (Initiator Test)".

- Configuration
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    (NUT:SGW-1)Identification Data field :
    3ffe: 501:ffff:100::,ffff:ffff:ffff:ffff::
    (TN:SGW-2)Identification Data field : ::(invalid value)
  - ✧ Identification Payload Format(IDcr, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-z addr	Net-v addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	::	Net-v addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

  * PHASE I
  For Phase-1 Sequence, refer "4.1Phase-1 Sequence (Initiator Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
 # Initiator(NUT)    Direction     Responder(TN)
(1)  HDR*,HASH(1),
     SA,Ni,IDci,IDcr; ========>
(2)                   <========  HDR*, HASH(2), SA, Nr,
                                 IDci, IDcr; <-----IDci data field: ::(invalid)
(3-A)HDR*,HASH(3)     ========> X           <-----Must not transmit
          or
(3-B)HDR*,HASH(1),N/D========>
                      Judgement
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify

Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the second message must not be accepted. The third message(3-A) must not be received (* or INVALID-ID-INFORMATION message(3-B) is received).
*option : if you want to check the retruned Notify message.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.3.1 ISAKMP Header format

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Responder cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 1(Security Association Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  indicates the type of exchange being used.
  (In this test, this field is set as 2(main mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission.
  |0|0|0|0|0|A|C|E|
- Message ID field
  During Phase 1 negotiations, the value MUST be set to 0.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  TN(HOST-1) transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination

  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).
(cookie is set to Responder cookie filed, Major version=1 and Minor version=0 , Flags field is correct and Message ID=0).

References:

RFC2408 : 3.1 ISAKMP Header Format
RFC2409 : 4. Introduction

7.3.2 Security Association Payload format

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or Transform(3) payload. Place the value of the Next Payload in the Next Payload field. (In this test, this field is set as 0).
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0). Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload. (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload. Implementations MUST support SIT_IDENTITY_ONLY.
  (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted.
And the second message's Security Association Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY
RFC2408 : 2.5.2 RESERVED Fields
3.4 Security Association Payload
5.3 Generic Payload Header Processing
5.4 Security Association Payload Processing

7.3.3 Proposal Payload format

Purpose:

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In Phase I, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In Phase I, this field contain the value "1".)
- Protocol-ID field
  All implementations within the IPSEC DOI MUST support PROTO_ISAKMP.
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.
  (In Phase I, this field is redundant and MAY be set to 0 or it MAY contain the transmitting entity's cookie.)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter

At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.1.1 PROTO_ISAKMP
RFC2408 : 2.5.2 RESERVED Fields

3.5 Proposal Payload
5.3 Generic Payload Header Processing
5.5 Proposal Payload Processing

7.3.4 Transform Payload format

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In responder, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
         <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message's Transform Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.2.1 KEY_IKE
RFC2408 : 2.5.2 RESERVED Fields
3.6 Transform Payload
5.3 Generic Payload Header Processing
5.6 Transform Payload Processing

7.3.5 Transform payload SA Attributes (DES,MD5,PSK,DH1)

Purpose:

IKE implementations MUST support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over default group number one.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DES-CBC, MD5, DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	DES	MD5	pre-shared key	1	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	DES	MD5	pre-shared key	1	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
         <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(DES:1,MD5:1,PSK:1,DH1:1) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction

7.3.6 Transform payload SA Attributes (DES,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DES-CBC)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(DES:1,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.3.7 Transform payload SA Attributes (AES-128,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- AES-128 in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CBC)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	AES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	AES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(AES:7,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

References:

RFC3602 : 5. IKE Interactions
          5.1. Phase 1 Identifier

7.3.8 Transform payload SA Attributes (3DES, MD5, PSK, DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - MD5 - Authentication via pre-shared keys. - MODP over group number two.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	MD5	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	MD5	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,MD5:1,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.3.9 Transform payload SA Attributes (3DES,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
            <IDENTITY PROTECTION EXCHANGE>
 #    Initiator(TN)    Direction     Responder(NUT)
(1)   HDR; SA          ========>
(2)                    <========        HDR; SA
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction
6.2 Second Oakley Group

7.3.10 Transform payload SA Attributes (3DES,SHA,RSA sign,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - RSA signatures. - MODP over group number two.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:1,SHA:2,RSA sign:3,DH2:2) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.3.11 Transform payload SA Attributes (3DES, SHA, PSK, DH1)

Purpose:

IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over default group number one.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH1:1) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction
          6.1 First Oakley Default Group

7.3.12 Transform payload SA Attributes (3DES, SHA, PSK, DH5)

Purpose:

IKE implementations support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number five.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH5:5) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction
RFC3526 : 2. 1536-bit MODP Group

7.3.13 Transform payload SA Attributes(3DES,SHA,PSK,DH14)

Purpose:

IKE implementations support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number fourteen.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH14:14) must be correct.
And must conform to above Configuration.

References:

RFC2409 : 4.Introduction

7.3.14 Multiple Transform Payloads check (Select proposal)

Purpose:

- An initiator MAY provide multiple proposals for negotiation; a responder MUST reply with only one
- The responder SHOULD retain the Proposal # field in the Proposal payload and the Transform # field in each Transform payload of the selected Proposal.
- IKE implementations SHOULD support the following attribute values

Parameter		Value
ISAKMP	SA Attributes	- 3DES in CBC mode - SHA - Authentication via pre-shared keys. - MODP over group number two.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I								
			Ex mode	Key Value	Trans #	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST		3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	1	65001	65001	65001	32768	8 Hour	SGW-2 addr
					2	3DES	SHA	pre-shared key	2	8 Hour	

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>
(2)                   <========       HDR; SA
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message that has only one proposal(3DES:5,SHA:2,PSK:1,DH2:2) and Transform # field = 2 must be returned. And must conform to above Configuration.

References:

RFC2408 : 4.1.1 Notation
          4.2 Security Association Establishment
RFC2409 : 3.2 Notation
          7.1 Phase 1 using Main Mode

7.3.15 Key Exchange Payload Format (DH1)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	1	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
(4)                  <========     HDR; KE; NONCE
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.3.16 Key Exchange Payload Format check(DH2)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
(4)                  <========     HDR; KE; NONCE
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.3.17 Key Exchange Payload Format check(DH5)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	5	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA
(3)  HDR; KE; NONCE  ========>
(4)                  <========    HDR; KE; NONCE
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.3.18 Key Exchange Payload Format (DH14)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	14	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
(4)                  <========     HDR; KE; NONCE
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information
   which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.3.19 Nonce Payload Format

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========       HDR; SA
(3)  HDR; KE; NONCE  ========>
(4)                  <========     HDR; KE; NONCE
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Nonce Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.13 Nonce Payload Processing
RFC2409 : 5. Exchanges

7.3.20 Encryption of ISAKMP payload

Purpose:

When communication is protected, all payloads following the ISAKMP header MUST be encrypted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**								
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
(6)                      <========      HDR*; IDir; HASH_R
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be accepted. And the sixth message must be encrypted and returned.And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format
RFC2409 : 3.2 Notation

7.3.21 Identification Payload Format

Purpose:

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, this field is set as 5(ID_IPV6_ADDR).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port ID field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, this value is NUT IPv6 address.)
- During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I								
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>
(6)                      <========      HDR*; IDir; HASH_R
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN

In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be accepted. And the sixth message's Identification Payload must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
        : 5.3 Generic Payload Header Processing
          5.8 Identification Payload Processing

7.3.22 HASH Payload Format

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH_R=prf(SKEYID,g^xr|g^xi|CKY-R|CKY-I|SAi_b|IDir_b))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
(6)                      <========     HDR*; IDir; HASH_R
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be accepted. And the sixth message's HASH Payload must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.11 Hash Payload Processing

7.3.23 Implementation of Main Mode with pre-shared key

Purpose:

Implementation of Main Mode with pre-shared key check.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR; SA              ========>
(2)                       <========       HDR; SA
              Judgement (Check *1)
(3)  HDR; KE; NONCE       ========>
(4)                       <========     HDR; KE; NONCE
              Judgement (Check *2)
(5)  HDR*; IDii; HASH_I   ========>
(6)                       <========     HDR*; IDir; HASH_R
              Judgement (Check *3)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the sixth message must be exchanged correctly.
  Check *1
    Security Association Payload Format must be base on description of RFC.
  Check *2
    Key Exchange and Nonce Payload Format must be base on description of RFC.
  Check *3
    Identification and Hash Payload Format must be base on description of RFC.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction
          5. Exchanges

7.3.24 cookie field

Purpose:

There is no relationship between the two SAs and the initiator and responder cookie pairs SHOULD be different.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	60 sec	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	60 sec	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <the first IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR; SA             ========>                       <---- Life Time = 60sec
(2)                      <========      HDR; SA          <---- Life Time = 60sec
                                                              #1:responder cookie
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I  ========>
(6)                      <========      HDR*; IDir; HASH_R
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) messages, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) messages, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) messages, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth (6) messages, the responder send identification information and the results of the agreed upon authentication function(hash function).

10sec after the first IDENTITY PROTECTION EXCHANGE,
negotiation of IKE(the second IDENTITY PROTECTION EXCHANGE) is started.

```
          <The second IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR; SA            ========>
(2)                     <========       HDR; SA      <---- #2:responder cookie
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
   In this message, initiator cookie is different from the first IDENTITY PROTECTION EXCHANGE's initiator cookie.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination

  Clean up SAD and SPD

Judgment:

In the first IDENTITY PROTECTION EXCHANGE, the first to the sixth message must be exchanged correctly. In the second IDENTITY PROTECTION EXCHANGE, The first message must be accepted. And 2th message's responder cookie(#2) is not same as the first IDENTITY PROTECTION EXCHANGE's responder cookie(#1).

References:

RFC2408 : 4.3 Security Association Modification

7.3.25 Certificate Request Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Type field
  Contains an encoding of the type of certificate requested
- Certificate Authority field
  Contains an encoding of an acceptable certificate authority for the type of certificate requested.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)     Direction      Responder(NUT)
(1)  HDR; SA           ========>
(2)                    <========        HDR; SA
(3)  HDR; KE; NONCE    ========>
(4)                    <========      HDR; KE; NONCE; CERT Req
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the second message must be exchanged correctly.
The third message must be accepted. And the fourth message's Certificate Request Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.10 Certificate Request Payload
5.3 Generic Payload Header Processing
5.10 Certificate Request Payload Processing

7.3.26 Signature Payload Format

Purpose:

Signature Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Signature Data field
  Data that results from applying the digital signature function to the ISAKMP message and/or state.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#    Initiator(TN)      Direction       Responder(NUT)
(1)  HDR; SA              ========>
(2)                       <========       HDR; SA
(3)  HDR; KE; NONCE       ========>
(4)                       <========      HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I    ========>
(6)                       <========      HDR*; IDir; SIG_R
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be accepted. And the sixth message's Signature Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.12 Signature Payload Processing

7.3.27 Certificate Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Encoding field
  This field indicates the type of certificate or certificate-related information contained in theCertificate Data field.
- Certificate Data field
  Actual encoding of certificate data

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)     Direction      Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE; CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I   ========>
(6)                      <========     HDR*; IDir; CERT; SIG_R
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload
6. Receive the sixth message from NUT

In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R. Additionally the responder send Certificate Request Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must be accepted. And the sixth message's Certificate Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.9 Certificate Payload

7.3.28 Implementation of Main Mode with RSA signatures

Purpose:

Implementation of Main Mode with RSA signatures check.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase I**							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)       Direction      Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
                Judgement (Check *1)
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
                Judgement (Check *2)
(5)  HDR*; IDii; SIG_I   ========>
(6)                      <========     HDR*; IDir; SIG_R
                Judgement (Check *3)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated
   digital signature algorithm applied to HASH_I.

6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function. The signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

- **Termination**

  Clean up SAD and SPD

Judgment:

The first to the sixth message must be exchanged correctly.

Check*1

Security Association Payload Format must be base on description of RFC.

Check*2

Key Exchange and Nonce Payload Format must be base on description of RFC.

Check*3

Identification and Signature Payload Format must be base on description of RFC.

And must conform to above Configuration.

References:

RFC2409 : 4. Introduction
5. Exchanges

7.3.29 Processing invalid ISAKMP Payload Length

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Length field = 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#Initiator(TN)   Direction   Responder(NUT)
(1) HDR; SA      ========>                  <-----Length field(ISAKMP header):
                                                              0(invalid)
(2-A)          X<========   HDR;KE;NONCE   <-----Must not transmit
                                or
(2-B)           <========    HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted.
And the second message must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.1 General Message Processing

7.3.30 Processing invalid Initiator Cookie field

Purpose:

Verify the Initiator and Responder "cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    In TEST PROCEDURE, Initiator Cookie field of the third message of IDENTITY PROTECTION EXCHANGE is set to 0(not same the first message's initiator cookie).
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA          ========>
(2)                   <========    HDR; SA
(3)  HDR; KE; NONCE    ========>             <-----Cookie field : 0(invalid
                                                    (not same as the first
                                                     message(1)'s cookie))
(4-A)               X <======== HDR*;KE;NONCE <-----Must not transmit
                                     or
(4-B)                 <========  HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   This message's Initiator Cookie is set to 0;
4. Receive the fourth message from NUT
   In the fourth message (4-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the second message must be exchanged correctly.
the third message must not be accepted. And the fourth message (4-A) must not be returned (* or INVALID-COOKIE message (4-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.3.31 Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Next Payload field = 127(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 # Initiator(TN)  Direction  Responder(NUT)
(1)  HDR; SA      ========>               <-----Next Payload field
                                                 (ISAKMP Header):127(invalid)
(2-A)         X <========  HDR; SA        <-----Must not trasnmit
                              or
(2-B)           <=======   HDR; N/D
            Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.3.32 Processing invalid Major Version fields (major 15, minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR- VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Major Version 15 (invalid value)
    Minor Version 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2-A)              X <========    HDR; SA    <-----Major Version : 15(invalid)
                                    or
(2-B)                <========    HDR; N/D   <-----Must not transmit
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MAJOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.3.33 Processing invalid Minor Version field (major 1,minor 15)

Purpose:

- Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:
  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.
  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  ✧ ISAKMP Header Format(HOST-2:Initiator)
  Major Version 1
  Minor Version 15 (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)  Direction   Responder(NUT)
(1)  HDR; SA         ========>               <-----Minor Version : 15(invalid)
(2-A)              X <========   HDR; SA     <-----Must not transmit
                                   or
(2-B)                <========   HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MINOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.3.34 Processing invalid Exchange Type field

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Exchange Type field = 31 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
# Initiator(TN)  Direction  Responder(NUT)
(1)  HDR; SA     ========>              <-----Exchange Type field:31(invalid)
(2-A)        X <========   HDR; SA     <-----Must not transmit
                             or
(2-B)          <========   HDR; N/D
             Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.3.35 Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate systemaudit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Flags field = |1|1|1|1|1|0|0|0| (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#  Initiator(TN) Direction  Responder(NUT)
(1) HDR; SA     ========>                <-----Flags field :|1|1|1|1|1|0|0|0|
                                                              (invalid value)
(2-A)        X <========     HDR; SA     <-----Must not transmit
                               or
(2-B)          <========     HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-FLAGS message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.3.36 Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values. If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Message ID field = 1 (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                     <-----Message ID field:1
                                                          (invalid value)
(2-A)              X <========       HDR; SA       <-----Must not transmit
                                        or
(2-B)                <========       HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned(* or INVALID-MESSAGE-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.3.37 Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ SA Payload Format(HOST-2:Initiator)
    RESERVED field : 1 (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                    <-----RESERVED field : 1
                                                         (SA, invalid value)
(2-A)                <========      HDR; SA       <-----Must not transmit
                                          or
(2-B)                <========      HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.3.38 Processing invalid Next Payload field

Purpose:

- This field MUST NOT contain the values for the Proposal or Transform payloads as they are considered part of the security association negotiation.
- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:
  - (a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.
  - (b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Next Payload field : 2 (Proposal Payload, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>                       <-----Next Payload field(SA) :
                                                                   2 (invalid value)
(2-A)              X <========        HDR; SA     <-----Must not transmit
                                         or
(2-B)                <========        HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
5.3 Generic Payload Header Processing

7.3.39 Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported. If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Domain of Interpretation field : 0xffffffff (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 # Initiator(TN)   Direction   Responder(NUT)
(1)  HDR; SA       ========>                <-----DOI field :
                                                  0xffffffff(invalid value)
(2-A)            X <========     HDR; SA    <-----Must not transmit
                                   or
(2-B)              <========     HDR; N/D
              Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or DOI-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.40 Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation field : 0x80000000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 # Initiator(TN)   Direction   Responder(NUT)
(1) HDR; SA        ========>                   <-----Situation field :
                                                      0x80000000(invalid value)
(2-A)            X <========    HDR; SA     <-----Must not transmit
                                   or
(2-B)              <========    HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message (2-A) must not be returned (* or SITUATION-NOT-SUPPORTED message (2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.41 Processing invalid proposal (Encryption Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	65000	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                     <-----Invalid proposal
(2-A)              X <========       HDR; SA       <-----Must not trasmit
                                        or
(2-B)                <========       HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.42 Processing invalid proposal (Hash Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	65000	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                    <-----Invalid proposal
(2-A)              X <========      HDR; SA       <-----Must not trasmit
                                       or
(2-B)                <========      HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.43 Processing invalid proposal (Authentication method)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	65000	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                    <-----Invalid proposal
(2-A)              X <========       HDR; SA      <-----Must not trasmit
                                        or
(2-B)                <========       HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.44 Processing invalid proposal (Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	32767	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                     <-----Invalid proposal
(2-A)              X <========       HDR; SA       <-----Must not trasmit
                                       or
(2-B)                <========       HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned(* NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.45 Processing invalid proposal (Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ SA attribute(HOST-2:Initiator, In Phase II)
    Life Type : 65000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                     <-----Invalid proposal
(2-A)              X <========      HDR; SA        <-----Must not trasmit
                                       or
(2-B)                <========      HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.3.46 IPSEC Situation Definition (SIT SECRECY)

Purpose:

If a responder does not support SIT_SECRECY, a SITUATION-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation : SIT_SECRECY
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction   Responder(NUT)
(1)  HDR; SA         ========>                   <-----Situation : SIT_SECRECY
(2-A)             X <========    HDR; SA        <-----Must not transmit if NUT
                                   or                doesn't support situation
(2-B)               <========    HDR; N/D                          SIT_SECRECY.
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

If Responder(NUT) doesn't support situation SIT_SECRECY, then the first message must not be accepted. (* And the second message(SITUATION-NOT-SUPPORTED Notification Payload)(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2407 : 4.2.2 SIT_SECRECY

7.3.47 IPSEC Situation Definition(SIT INTEGRITY)

Purpose:

If a responder does not support SIT_INTEGRITY, a SITUATION-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation : SIT_INTEGRITY
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>
(2-A)               X <========  HDR; SA        <-----Must not transmit if NUT
                                   or                doesn't support situation
 (2-B)                <======== HDR; N/D                        SIT_INTEGRITY.
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

If Responder(NUT) doesn't support situation SIT_INTEGRITY, then the first message must not be accepted. (* And the second message(SITUATION-NOT-SUPPORTED Notification Payload)(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2407 : 4.2.3 SIT_INTEGRITY

7.3.48 Processing invalid Protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Initiator)
    Protocol-ID field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                  <-----Protocol-ID field : 248
                                                                (invalid value)
(2-A)              X <========     HDR; SA      <-----Must not transmit
                                     or
(2-B)                <========     HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PROTOCOL-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.3.49 Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Initiator)
    SPI field : SPI value is set as 1 (not same cookie value, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 # Initiator(TN)  Direction  Responder(NUT)
(1) HDR; SA       ========>                  <-----SPI field : 1(invalid value)
(2-A)          X <========    HDR; SA        <-----Must not transmit
                                or
(2-B)             <=======      HDR; N/D
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-SPI message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.3.50 Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Initiator)
    Number of Transforms field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>              <-----Number of Transforms field:
                                                          0(invalid value)
(2-A)              X <========     HDR; SA  <-----Must not transmit
                                     or
(2-B)                <========     HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.3.51 Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Transform Payload Format(HOST-2:Initiator)
    Transform-ID field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                  <-----Transform-ID field : 248
                                                               (invalid value)
(2-A)              X <========      HDR; SA    <-----Must not transmit
                                       or
(2-B)                <========      HDR; N/D
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A)
must not be returned (* or INVALID-TRANSFORM-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.3.52 Processing invalid Transform Payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Initiator)
    SA Attributes field : not set (see below)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST						SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>                    <-----SA Attributes field :
                                                           not set(invalid)
(2-A)              X <========       HDR; SA      <-----Must not transmit
                                         or
(2-B)                <========       HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.3.53 Multiple Transform Payloads check (reject proposal)

Purpose:

The receiving entity MUST select a single transform for each protocol in a proposal or reject the entire proposal.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I								
			Ex mode	Key Value	Trans #	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST		3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	1	65001	65001	65001	32768	8 Hour	SGW-2 addr
					2	65002	65002	65002	32769	8 Hour	

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
            <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR; SA          ========>                        <-----Multiple invalid
                                                              transform payloads
(2)                 X <========       HDR; SA          <-----Must not transmit
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2) must not be returned.

References:

RFC2408 : 4.2 Security Association Establishment

7.3.54 Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Key Exchange Payload Format(HOST-2:Initiator)
    Key Exchange Data field : 0(1byte) (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)   Direction    Responder(NUT)
(1)  HDR; SA         ========>
(2)                  <========      HDR; SA
(3)  HDR; KE; NONCE  ========>                <-----Key Exchange Data field:0
                                                        (1byte)(invalid value)
(4-A)              X <========      HDR; KE; NONCE <-----Must not transmi
                                      or
(4-B)                <========      HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth message (4-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the second message must be exchanged correctly.
The third message must not be accepted. And the fourth message(4-A) must not be returned (* or INVALID-KEY-INFORMATION message(4-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.7 Key Exchange Payload Processing

7.3.55 Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Identification Payload Format(HOST-2:Initiator)
    ID Type field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#Initiator(TN)    Direction  Responder(NUT)
(1)HDR; SA        ========>
(2)               <========  HDR; SA
(3)HDR;KE;NONCE   ========>
(4)               <========HDR;KE;NONCE
(5)HDR*;IDii;HASH_I========>          <-----ID Type field:248(invalid value)
(6-A)           X <========HDR*;IDir;HASH_R<-----Must not transmit
                                  or
(6-B)             <========HDR*;HASH(1);N/D
                               (HDR; N/D)
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association,Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth message (6-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-ID-INFORMATION message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.8 Identification Payload Processing

7.3.56 Not include Identification Payload

Purpose:

All IPSEC DOI implementations MUST support SIT_IDENTITY_ONLY by including an Identification Payload in at least one of the Phase I Oakley exchanges and MUST abort any association setup that does not include an Identification Payload.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - Initiator(TN) does not send ID payload by the the fifth message.
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
# Initiator(TN) Direction Responder(NUT)
(1) HDR; SA      ========>
(2)             <========  HDR; SA
(3)HDR;KE;NONCE ========>
(4)             <========  HDR; KE; NONCE
(5)HDR*; HASH_I ========>                   <----not include ID payload(invalid)
(6)           X <======== HDR*;IDir;HASH_R <----must not transmit
              Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
   In this test, TN does not send identification information(ID payload).
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message must not be returned.

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY

7.3.57 Invalid Identification Payload receive

Purpose:

During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500. If an implementation receives any other values, this MUST be treated as an error and the security association setup MUST be aborted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator(TN)'s protocol ID fields of ID payload is set to TCP. (invalid value)
  - ✧ Initiator(TN)'s port fields of ID payload is set to 300. (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>                    <-----ID protocol/port :
                                                       TCP/300(invalid value)
(6)                    X <======== HDR*; IDir; HASH_R <-----Must not transmit
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth (6) message, the responder send identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message must not be returned.

References:

RFC2407: 4.6.2 Identification Payload Content
RFC2408: 5.8 Identification Payload Processing

7.3.58 Processing invalid Hash payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Initiator)
    Hash Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
           <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)    Direction    Responder(NUT)
(1)  HDR; SA        ========>
(2)                 <========     HDR; SA
(3)  HDR; KE; NONCE ========>
(4)                <========  HDR; KE; NONCE
(5)HDR*;IDii;HASH_I ========>                <----Hash Data field : not include
                                                          this field (invalid)
(6-A)           X <======== HDR*;IDir;HASH_R <-----Must not transmit
                                   or
(6-B)              <======== HDR*; HASH(1); N/D
                             (HDR; N/D)
              Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.

5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).

6. Receive the sixth message from NUT
   In the sixth message (6-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-HASH-INFORMATION message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.3.59 Processing invalid Hash Data field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Hash Payload Format(HOST-2:Initiator)
    Hash Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main	IKE-TEST	3DES	SHA	pre-shared key	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)       Direction     Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========       HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========     HDR; KE; NONCE
(5)  HDR*; IDii; HASH_I ========>                  <-----Hash Data field : 0
                                                                  (invalid)
(6-A)                  X <========    HDR*; IDir; HASH_R <-----Must not transmit
                                                 or
(6-B)                    <========     HDR*; HASH(1); N/D
                                        (HDR; N/D)
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function(hash function).
6. Receive the sixth message from NUT
   In the sixth message (6-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not accepted. And the sixth message(6-A) must not be returned (* or AUTHENTICATION-FAILED message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.3.60 Processing invalid Signature Payload

Purpose:

Determine if the Signature is supported. If the Signature determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SIGNATURE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key.
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Initiator)
    Signature Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction    Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========    HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========  HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I  ========>               <-----Signature Data field :
                                                       not include this field
                                                                    (invalid)
(6-A)                  X <========  HDR*; IDir; SIG_R <----Must not transmit
                                        or
(6-B)                    <========  HDR*; HASH(1); N/D
                                     (HDR; N/D)
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
6. Receive the sixth message from NUT
   In the sixth message (6-B), the responder indicates either an ISAKMP Notify

Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned(* or INVALID-SIGNATURE message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

7.3.61 Processing invalid Signature Data field

Purpose:

Perform the Signature function as outlined in the DOI and/or Key Exchange protocol documents. If the Signature function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Initiator)
    Signature Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR; SA             ========>
(2)                      <========        HDR; SA
(3)  HDR; KE; NONCE      ========>
(4)                      <========      HDR; KE; NONCE
(5)  HDR*; IDii; SIG_I  ========>               <---Signature Data field : 0
                                                                   (invalid)
(6-A)                  X <========      HDR*; IDir; SIG_R <---Must not transmit
                                            or
(6-B)                    <========      HDR*; HASH(1); N/D
                                        (HDR; N/D)
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
6. Receive the sixth message from NUT

In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first to the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or AUTHENTICATION-FAILED message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

7.3.62 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    Cert Encoding : 255 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)     Direction    Responder(NUT)
(1)  HDR; SA          ========>
(2)                   <========     HDR; SA
(3)  HDR; KE; NONCE    ========>
(4)                    <========   HDR; KE; NONCE; CERT Req
(5)  HDR*; IDii; CERT;
      CERT Req; SIG_I   ========>                <-----Cert Encoding Type fild:
                                                              255 (invalid)
(6)                    <========   HDR*; HASH(1); N/D
                                     (HDR; N/D)
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload
6. Receive the sixth message from NUT
   In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
    Clean up SAD and SPD

Judgment:

The first and the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-CERT-ENCODING message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.3.63 Processing invalid Certificate Authority field

Purpose:

Determine if the Certificate Authority is supported for the specified Certificate Encoding. If the Certificate Authority is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE AUTHORITY, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-AUTHORITY message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    Certificate Authority field: 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	**Key Value**	**Enc Alg**	**Hash Alg**	**Auth Method**	**DH Group**	**PH1 Lt**	**IDx**
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction    Responder(NUT)
(1)  HDR; SA            ========>
(2)                     <========     HDR; SA
(3)  HDR; KE; NONCE     ========>
(4)                     <========HDR;KE;NONCE;CERT Req
(5) HDR*; IDii; CERT;
   CERT Req; SIG_I       ========>               <-----Cert Data field: 0
(invalid)
(6)                     <========     HDR*; HASH(1); N/D
                                       (HDR; N/D)
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload

6. Receive the sixth message from NUT
   In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-CERT-AUTHORITY message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.3.64 Processing invalid Certificate Type with Certificate Authority

Purpose:

Process the Certificate Request. If a requested Certificate Type with the specified Certificate Authority is not available, then the payload is discarded and the following actions are taken:

(a) The event, CERTIFICATE-UNAVAILABLE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the CERTIFICATE-UNAVAILABLE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    Certificate Authority field: Distinguish Name
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN) Direction  Responder(NUT)
(1) HDR; SA       ========>
(2)              <========   HDR; SA
(3)HDR; KE; NONCE ========>
(4)              <========HDR;KE;NONCE;CERT Req
(5)HDR*;IDii;CERT;
   CERT Req; SIG_I========>                    <-----Certificate Data field:
(6)              <======== HDR*;HASH(1);N/D          The value which is not
                           (HDR; N/D)             available for Certificate
              Judgement (Check *1)                                Authority
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload
6. Receive the sixth message from NUT

In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The first and the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message must not be returned (*or CERTIFICATE-UNAVAILABLE message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

7.3.65 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is not supported, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Initiator)
    Cert Encoding field : 255 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
#   Initiator(TN)      Direction    Responder(NUT)
(1)  HDR; SA           ========>
(2)                    <========    HDR; SA
(3)  HDR; KE; NONCE    ========>
(4)                    <======== HDR;KE;NONCE;CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I ========>                  <-----Cert Encoding Type fild:
(6)                    <======== HDR*;HASH(1);N/D                 255(invalid)
                                        (HDR; N/D)
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send Certificate and Certificate Request Payload
6. Receive the sixth message from NUT
   In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-CERT-ENCODING message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

7.3.66 Processing invalid Certificate Data field

Purpose:

Process the Certificate Data field. If the Certificate Data is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERTIFICATE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Digital Signature (RSA))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Initiator)
    Certificate Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

Machine	Src	Dest	Phase I							
			Ex mode	Key Value	Enc Alg	Hash Alg	Auth Method	DH Group	PH1 Lt	IDx
SGW-1	SGW-1 addr	SGW-2 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-1 addr
SGW-2	SGW-2 addr	SGW-1 addr	Main		3DES	SHA	RSA signatures	2	8 Hour	SGW-2 addr

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
          <IDENTITY PROTECTION EXCHANGE>
 #   Initiator(TN)      Direction   Responder(NUT)
(1)  HDR; SA            ========>
(2)                     <========    HDR; SA
(3)  HDR; KE; NONCE     ========>
(4)                     <======== HDR;KE;NONCE;CERT Req
(5)  HDR*; IDii; CERT;
       CERT Req; SIG_I ========>                 <----Certificate Encoding
(6)                     <======== HDR*;HASH(1);N/D         field : 0 (invalid)
                                       (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.
3. Send the third message from TN
   In the third (3) message, the initiator send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
4. Receive the fourth message from NUT
   In the fourth (4) message, the responder send keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks.
   Additionally the responder send Certificate Request Payload.
5. Send the fifth message from TN
   In the fifth (5) message, the initiator send identification information and the results of the agreed upon authentication function. The signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.
   Additionally the initiator send invalid Certificate and Certificate Request Payload
6. Receive the sixth message from NUT
   In the sixth message (6), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first and the fourth message must be exchanged correctly.
The fifth message must not be accepted. And the sixth message(6-A) must not be returned (* or INVALID-CERTIFICATE message(6-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

7.4.1 Encryption of ISAKMP payload

Purpose:

The information exchanged along with Quick Mode MUST be protected by the ISAKMP SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

＊ PHASE II

```
                          <QUICK MODE>
 #    Initiator(TN)       Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr;   ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message must be encrypted and returned.And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format
RFC2409 : 3.2 Notation
          5.5 Phase 2 - Quick Mode

7.4.2 Position of payload

Purpose:

In Quick Mode, a HASH payload MUST immediately follow the ISAKMP header and a SA payload MUST immediately follow the HASH.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #    Initiator(TN)       Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which has correct position of payload must be returned.
And must conform to above Configuration.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.4.3 ISAKMP Header Format check(Phase II)

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Responder cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 8(Hash Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  indicates the type of exchange being used.
  (In this test, this field is set as 32(Quick mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission. |0|0|0|0|0|A|C|E|
- Message ID field
  Unique Message Identifier used to identify protocol state during Phase 2 negotiations.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

```
  The test sequence is following.
* PHASE II
                         <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 3.1 ISAKMP Header Format
5.2 ISAKMP Header Processing

7.4.4 HASH Payload Format (Phase II)

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH(2)=prf(SKEYID_a,M-ID|Ni_b|SA|Nr[|KE][|IDci|IDcr))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
   And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.
   HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message's HASH Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.4.5 Security Association Payload format (Phase II)

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or ransform(3) payload. Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0). Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload. (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload. Implementations MUST support SIT_IDENTITY_ONLY. (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT

   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message's Security Association Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY
RFC2408 : 2.5.2 RESERVED Fields
          3.4 Security Association Payload

7.4.6 Proposal Payload format (Phase II)

Purpose:

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0"
  (In this test, value is 0).
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In this test, this field contain the value "1".)
- Protocol-ID field
  Specifies the protocol identifier for the current negotiation.
  (In this test, this field contain the value "3"(PROTO_IPSEC_ESP))
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter

    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>

 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>

(2)                     <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT

   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads.

And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 2.5.2 RESERVED Fields
3.5 Proposal Payload
5.3 Generic Payload Header Processing
5.5 Proposal Payload Processing

7.4.7 Transform Payload format (Phase II)

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0"
  (In this test, value is 0).
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In this test, this field contain "3"(ESP_3DES))

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
#   Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message's Transform Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2408 : 2.5.2 RESERVED Fields
3.6 Transform Payload
5.3 Generic Payload Header Processing
5.6 Transform Payload Processing

7.4.8 Transform payload SA Attributes (ESP_DES, HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3. (see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support DES-CBC, HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <QUICK MODE>
#    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message which has ESP_DES and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).And must conform to above Configuration.

References:

RFC2407 : 4.4.4.2 ESP_DES
          4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.9 Transform payload SA Attributes (ESP_3DES,HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI are strongly encouraged tosupport ESP_3DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I

For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

＊PHASE II

```
                         <QUICK MODE>
#   Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which has ESP_3DES and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.3 ESP_3DES

4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.10 Transform payload SA Attributes (ESP_3DES,HMAC-SHA)

Purpose:

- All implementations within the IPSEC DOI are strongly encouraged to support ESP_3DES along with the Auth(HMAC-MD5) attribute.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message which has ESP_3DES and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).And must conform to above Configuration.

References:

RFC2407 : 4.4.4.3 ESP_3DES
          4.5 IPSEC Security Association

RFC2408 : 3.3 Data Attributes

7.4.11 Transform payload SA Attributes (ESP_3DES, AES-XCBC-MAC)

Purpose:

- AES-128 in CBC mode for HMAC function SHOULD be supported
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3. (see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ADS-XCBC-MAC)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	AES-XCBC-MAC	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	AES-XCBC-MAC	8 Hour	Net-v addr	Net-z addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message which has ESP_3DES and Auth(AES-XCBC-MAC) attribute must be received and must be base on description of RFC (see above Verification Points). And must conform to above Configuration.

References:

RFC3566 : 6. IANA Considerations
RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.12 Transform payload SA Attributes (ESP_AES(128bit),HMAC-SHA)

Purpose:

- AES-128 in CBC mode [RFC3602] SHOULD be supported
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CBC (128bit))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
＊PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
In Phase II, the first message must be accepted. And the second message which has ESP_AES and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC3602 : 5. IKE Interactions
RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.13 Transform payload SA Attributes (ESP_NULL,HMAC-MD5)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL, HMAC-MD5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-MD5	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which has ESP_NULL and Auth(HMAC-MD5) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.11 ESP_NULL
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.14 Transform payload SA Attributes (ESP_NULL,HMAC-SHA)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                       <QUICK MODE>
#   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which has ESP_NULL and Auth(HMAC-SHA) attribute must be received and must be base on description of RFC (see above Verification Points).

References:

RFC2407 : 4.4.4.11 ESP_NULL
           4.5 IPSEC Security Association Attributes

7.4.15 Transform payload SA Attributes (ESP_NULL,AES-XCBC-MAC)

Purpose:

- All implementations within the IPSEC DOI MUST support ESP_NULL.
- When negotiating ESP without confidentiality, the Auth Algorithm attribute MUST be included in the proposal and the ESP transform ID must be ESP_NULL.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP_NULL, AES-XCBC-MAC)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	AES-XCBC-MAC	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_NULL	Tunnel	AES-XCBC-MAC	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which has ESP_NULL and Auth(AES-XCBC-MAC) attribute must be received and must be base on description of RFC (see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.4.4.11 ESP_NULL
4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.16 ESP without Authentication Algorithm(ESP_DES)

Purpose:

- When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication), DES-CBC)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Transform Payload Format(HOST-2:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                      <QUICK MODE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points).

And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.17 ESP without Authentication Algorithm(ESP_3DES)

Purpose:

- When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3. (see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                         <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attributes
RFC2408 : 3.3 Data Attributes

7.4.18 ESP without Authentication Algorithm(ESP_AES)

Purpose:

- When negotiating ESP without authentication, the Auth Algorithm attribute MUST NOT be included in the proposal.
- Attributes described as basic MUST NOT be encoded as variable.
- An SA Life Duration attribute MUST always follow an SA Life Type which describes the units of duration.
- The SA Attributes SHOULD be represented using the Data Attributes format described in section 3.3.(see reference)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication), AES-CBC (128bit))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - ✧ Transform Payload Format(HOST-2:initiator)
    SA Attribute : not include Auth Algorithm
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel		8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_AES	Tunnel		8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <QUICK MODE>
#   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>

(2)                      <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which does not include Auth Algorithm must be received and must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2407 : 4.5 IPSEC Security Association Attribu
RFC2408 : 3.3 Data Attributes

7.4.19 Multiple Proposal and Transform Payloads (select proposal)

Purpose:

- An initiator MAY provide multiple proposals for negotiation; a responder MUST reply with only one.
- The receiving entity MUST select a single transform for each protocol in a proposal or reject the entire proposal.
- When responding to a Security Association payload, the responder MUST send a Security Association payload with the selected proposal, which may consist of multiple Proposal payloads and their associated Transform payloads.
  Each of the Proposal payloads MUST contain a single Transform payload associated with the Protocol.
  The responder SHOULD retain the Proposal # field in the Proposal payload and the Transform # field in each Transform payload of the selected Proposal.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II									
			Prop #	Proto ID	Trans #	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr		PROTO_IPSEC_ESP		ESP_3DES	Tunnel	HMAC-SHA	8 Hour			
SGW-2	SGW-2 addr	SGW-1 addr	1	PROTO_IPSEC_AH	1	249	Tunnel	61440	8 Hour	Net-v addr	Net-z addr	any
					2	250	Tunnel	61441	8 Hour			
			2	PROTO_IPSEC_ESP	1	249	Tunnel	61440	8 Hour			
						ESP_3DES	Tunnel	HMAC-SHA	8 Hour			

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
#    Initiator(TN)        Direction        Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                         <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except

the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II ,the first message must be accepted.
The second message that has two Proposal(Proposal # = 2) and only one Transform (Transform # = 2) (attribute is ESP_3DES,Transport, HMAC-SHA, 8 Hour) must be returned.

References:

RFC2408 : 4.1.1 Notation
          4.2 Security Association Establishment
RFC2409 : 3.2 Notation

7.4.20 enable PFS with DH1

Purpose:

- DH Group
  Oakley implementations MUST support a MODP group with the following prime and generator. This group is assigned id 1 (one).
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode.While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                      <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                     <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.

And the second message which has KE payload and DH1 as SA attribute must be received.And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
6.1 First Oakley Default Group

7.4.21 enable PFS with DH2

Purpose:

- DH Group
  IKE implementations SHOULD support a MODP group with the following prime and generator. This group is assigned id 2 (two).
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode. While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)       Direction        Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                       <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly. In Phase II, the first message must be accepted. And the second message which has KE payload and DH2 as SA attribute must be received.And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
6.2 Second Oakley Group

7.4.22 enable PFS with DH5

Purpose:

- DH Group
  IKE implementations support a 1536 bit MODP group.
  This group is assigned id 5.
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode.While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                     <QUICK MODE>
 #   Initiator(TN)     Direction      Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                     <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.

And the second message which has KE payload and DH5 as SA attribute must be received.And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
RFC3526 : 2. 1536-bit MODP Group

7.4.23 enable PFS with DH14

Purpose:

- DH Group
  IKE implementations support a 2048 bit MODP group.
  This group is assigned id 14.
- PFS
  For PFS to exist the key used to protect transmission of data MUST NOT be used to derive any additional keys, and if the key used to protect transmission of data was derived from some other keying material, that material MUST NOT be used to derive any more keys.
- KE payload
  An optional Key Exchange payload can be exchanged to allow for an additional Diffie-Hellman exchange and exponentiation per Quick Mode. While use of the key exchange payload with Quick Mode is optional it MUST be supported.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH14)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
#   Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                      <========    HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.

And the second message which has KE payload and DH14 as SA attribute must be received. And must conform to above Configuration.

References:

RFC2409 : 3.3 Perfect Forward Secrecy
5.5 Phase 2 - Quick Mode
RFC3526 : 3. 2048-bit MODP Group

7.4.24 Key Exchange Payload Format (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH1)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	1	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                      <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.4.25 Key Exchange Payload Format(DH2) (Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1), SA,
      Ni, KE ,IDci, IDcr;========>
(2)                       <========     HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
           5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.4.26 Key Exchange Payload Format check(DH5)(Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH5)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	5	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>
(2)                      <========      HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.

In Phase II,the first message must be accepted.And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.4.27 Key Exchange Payload Format (DH14)(Phase II)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS, DH14)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	14	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1), SA,
      Ni, KE ,IDci, IDcr;========>
(2)                       <========      HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni,minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I,messages must be exchanged correctly.
In Phase II,the first message must be accepted.

And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

7.4.28 Nonce Payload Format (Phase II)

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  ＊ PHASE Ⅰ
  For Phase-1 Sequence, refer ″4.2Phase-1 Sequence (Responder Test)″

Procedure:

The test sequence is following.

```
＊ PHASE ＩＩ
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase Ｉ, messages must be exchanged correctly.
In Phase ＩＩ,the first message must be accepted.
And the second message's Nonce Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
           5.13 Nonce Payload Processing
RFC2409 : 5. Exchanges

7.4.29 Key Exchange Payload w/o PFS

Purpose:

If PFS is not needed, and KE payloads are not exchanged

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".

  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 # Initiator(TN)       Direction         Responder(NUT)
(1)HDR*, HASH(1),
   SA,Ni,IDci,IDcr;   ========>
(2)                  <======== HDR*,HASH(2),SA,Nr,IDci,IDcr;<--- must not send
                Judgement (Check *1)                             KE payload.
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted. And the second message which must not has KE payload, must be received and must be base on description of RFC (see above Verification Points). And must conform to above Configuration.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode

7.4.30 Identification Payload Format (Phase II,tunnel mode to SGW)

Purpose:

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, this field is set as 6(ID_IPV6_ADDR_SUBNET).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, IDci's this field has
  3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::(Net-v network address).
  IDcr's this field has 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::
  (Net-z network address).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)

Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field : 3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::

✧ Identification Payload Format(IDcr, In Phase II)
Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field : 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::

✧ Initiator and Responder IKE parameter
At least, following parameter must be included in proposal.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
 #    Initiator(TN)        Direction        Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                        <========      HDR*,HASH(2),SA,Nr,IDci,IDcr;
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1)

is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must be accepted.And the second message which Identification Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
5.3 Generic Payload Header Processing
5.8 Identification Payload Processing
RFC2409 : 5.5 Phase 2 - Quick Mode

7.4.31 Identification Payload Format (Phase II,tunnel mode to HOST)

Purpose:

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, IDci's this field is set as 5(ID_IPV6_ADDR).
  IDcr's this field is set as 6(ID_IPV6_ADDR_SUBNET).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, IDci's this field has 3ffe:501:ffff:103::11(TN(HOST-2) IPv6 address).IDcr's this field has
  3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::(Net-z network address).)

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 4 Topology for SGW vs. HOST (Responder Test)".
- **Configuration**
  ✧ Identification Payload Format(IDci, In Phase II)
  Identification Type field : 5(ID_IPV6_ADDR)

Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field : 3ffe:501:ffff:103::11

✧ Identification Payload Format(IDcr, In Phase II)
Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
Protocol ID field : 0(any)
Port field : 0(any)
Identification Data field : 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::

✧ Initiator and Responder IKE parameter
At least, following parameter must be included in proposal.

For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	Net-z addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                      <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1)

is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I,messages must be exchanged correctly.
In Phase II,the first message must be accepted.And the second message which Identification Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
           5.3 Generic Payload Header Processing
           5.8 Identification Payload Processing
RFC2409 : 5.5 Phase 2 - Quick Mode

7.4.32 set Commit Bit(CONNECTED Notify Message)

Purpose:

If set(1), the entity which did not set the Commit Bit MUST wait for an Informational Exchange containing a Notify payload (with the CONNECTED Notify Message) from the entity which set the Commit Bit.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Commit Bit)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator(TN)'s Commit Bit of ISAKMP header is set to 1 in Phase II.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(TN)       Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                        <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)       ========>                              <--- Commit Bit = 1
(4)   HDR*; HASH(1), N/D ========>                               <--- Commit Bit = 1
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

4. Send the fourth message from TN
   In the fourth message (4), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload. In this case, the initiator send CONNECTED Notify Message.

＊ IPsec transmission
Send Echo Request from HOST-1 to HOST-2 before the CONNECTED Notify Message(The forth messege in Phase II)

```
 # Initiator(TN)  Direction  Responder(NUT)
(1)                          IP_HDR; ESP*;
                  <======= ICMP(Echo request) <-- HOST-1 Send Echo request before
                 Judgement (Check *1)              the CONNECTED Notify Message
                                                 (The forth messege in Phase II)
```

1. Receive the first message from NUT
   In the first message (1), Responder(NUT) forward Echo request from HOST-1(TN) to Initiator(TN) with IPsec SA.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
And NUT wait for an Informational Exchange containing a Notify payload(with the CONNECTED Notify Message).
Before NUT recive the CONNECTED Notify Message, HOST-1 send Echo Request to HOST-2, but this Echo Request must not be foward before SGW-2(initiator) send the CONNECTED Notify Message.
After NUT revive the CONNECTED Notify Message, NUT must foward Echo Request with IPsec SA.
And must conform to above Configuration.

References:

RFC2408 : 3.1 ISAKMP Header Format

7.4.33 Implementation of Quick Mode (ESP_3DES(Tunnel mode to SGW))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                       <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                 Judgement (Check *1)
(3)  HDR*, HASH(3)        ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
* IPsec transmission

 #   Initiator(TN)      Direction       Responder(NUT)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
                 Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT) with IPsec SA. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1 : Hash, Security Association, Nonce, Identification Payload Format
             must be base on description of RFC.
In IPsec SA transmission, the first message must be forwarded to HOST-1(TN).
  Check *2 : NUT must forward Echo Reply to HOST-1.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.4.34 Implementation of Quick Mode (ESP_3DES and HMAC-SHA(Tunnel mode to SGW))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

＊ PHASE II

```
                        <QUICK MODE>
 #    Initiator(TN)      Direction        Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
                  Judgement (Check *1)
(3)   HDR*, HASH(3)      ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ IPsec transmission

```
 #    Initiator(TN)      Direction        Responder(NUT)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)  ========>
                  Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT) with IPsec SA. And NUT(SGW-1) forward decrypted Echo request

to HOST-1(TN).

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1 : Hash, Security Association, Nonce, Identification Payload Format
             must be base on description of RFC.
In IPsec SA transmission, the first message must be forwarded to HOST-1(TN).
  Check *2 : NUT must forward Echo Reply to HOST-1.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.4.35 Implementation of Quick Mode (ESP_3DES(Tunnel mode to HOST))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support ESP (without Authentication))

Initialization:

- Network Topology
  Refer the topology "Figure 4 Topology for SGW vs. HOST (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	HOST-2 addr	Net-z addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel		8 Hour	HOST-2 addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
                   Judgement (Check *1)
(3)   HDR*, HASH(3)       ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #    Initiator(TN)      Direction       Responder(NUT)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>
                   Judgement (Check *2)
```

1. Send the first message from TN

In the first message(1), initiator(TN) send Echo request from to responder(NUT) with IPsec SA. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1 : Hash, Security Association, Nonce, Identification Payload Format
  must be base on description of RFC.
In IPsec SA transmission, the first message must be forwarded to HOST-1(TN).
  Check *2 : NUT must forward Echo Reply to HOST-1.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.4.36 Implementation of Quick Mode (ESP_3DES and HMAC-SHA(Tunnel mode to HOST))

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 4 Topology for SGW vs. HOST (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	HOST-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	Net-z addr	any
HOST -2	HOST -2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                           <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                        <========     HDR*, HASH(2), SA, Nr, IDci, IDcr;
                   Judgement (Check *1)
(3)   HDR*, HASH(3)        ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #    Initiator(TN)      Direction       Responder(NUT)
(1)   IP_HDR; ESP*;
      ICMP(Echo request)   ========>
                   Judgement (Check *2)
```

1. Send the first message from TN

In the first message (1), initiator(TN) send Echo request to responder(NUT) with IPsec SA. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1 : Hash, Security Association, Nonce, Identification Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be forwarded to HOST-1(TN).
  Check *2 : NUT must forward Echo Reply to HOST-1.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.4.37 Implementation of Quick Mode with PFS

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support PFS)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**DH Group**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE, IDci, IDcr;========>
(2)                      <========      HDR*, HASH(2), SA, Nr, KE, IDci, IDcr;
                  Judgement (Check *1)
(3)  HDR*, HASH(3)       ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

```
 * IPsec transmission

 #   Initiator(TN)      Direction       Responder(NUT)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)   ========>
                  Judgement (Check *1)
```

1. Send the first message from TN

In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT) with IPsec SA. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly.
  Check *1 : Hash, Security Association, Nonce, Key Exchange, Identification
             Payload Format must be base on description of RFC.
In IPsec SA transmission, the first message must be forwarded to HOST-1(TN).
  Check *2 : NUT must forward Echo Reply to HOST-1.
And must conform to above Configuration.

References:

RFC2409 : 5. Exchanges

7.4.38 Using new SA for outbound traffic

Purpose:

A protocol implementation SHOULD begin using the newly created SA for outbound traffic and SHOULD continue to support incoming traffic on the old SA until it is deleted or until traffic is received under the protection of the newly created SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <the first QUICK MODE>
#    Initiator(TN)       Direction        Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)      ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ PHASE II

the second QUICK MODE is performed after 10sec from establishment of the first IPsec SA(1st QUICK MODE).

```
                         <the second QUICK MODE>
#   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>
(2)                     <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)  HDR*, HASH(3)      ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ IPsec transmission

```
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  IP_HDR; ESP*;
     ICMP(Echo request)  ========>
(2)                     <========        IP_HDR; ESP*; ICMP(Echo reply)
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT) using IPsec SA that established by the second QUICK MODE.

And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

2. Receive the second message from NUT
   In the second message (2), responder(NUT) forward encrypted Echo reply from HOST-1(TN) to initiator(TN) using IPsec SA that established by the second QUICK MODE.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second IPsec SA is established correctly.
In IPsec SA transmission, the first message using the second IPsec SA must be accepted.And the second message using the second IPsec SA must be returned.
And must conform to above Configuration.

References:

RFC2408 : 4.3 Security Association Modification

7.4.39 Accept both old and new SA for incoming traffic

Purpose:

A protocol implementation SHOULD begin using the newly created SA for outbound traffic and SHOULD continue to support incoming traffic on the old SA until it is deleted or until traffic is received under the protection of the newly created SA.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	60 sec	Net-v addr	Net-z addr	any

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                      <the first QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)      ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

* PHASE II

the second QUICK MODE is performed after 10sec from establishment of the first IPsec SA(1st QUICK MODE).

```
                      <the second QUICK MODE>
#    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                      <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)      ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

＊ IPsec transmission

```
 #   Initiator(TN)    Direction    Responder(NUT)
(1)IP_HDR; ESP*;
  ICMP(Echo request)   ========>                 <----This message is sent before
                                                          the first SA expires.
(2)                   <======== IP_HDR; ESP*; ICMP(Echo reply)
(3)IP_HDR; ESP*;
  ICMP(Echo request)   ========>
(4)                   <======== IP_HDR; ESP*; ICMP(Echo reply)
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT) using IPsec SA that established by the first QUICK MODE. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

2. Receive the second message from NUT
   In the second message (2), responder(NUT) forward encrypted Echo reply from HOST-1(TN) to initiator(TN).

3. Send the third message from TN
   In the third message (3), initiator(TN) forward Echo request from HOST-2(TN)

to responder(NUT) using IPsec SA that established by the second QUICK MODE. And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).

4. Receive the fourth message from NUT
   In the fourth message (4), responder(NUT) forward encrypted Echo reply from HOST-1(TN) to initiator(TN).

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second IPsec SA is established correctly.
In IPsec SA transmission, the first message using the first IPsec SA must be accepted.And the second message using the second IPsec SA must be returned.
The third message using the second IPsec SA must be accepted.
And the fourth message using the second IPsec SA must be returned.
And must conform to above Configuration.

References:

RFC2408 : 4.3 Security Association Modification

7.4.40 Increasing Sequence Number

Purpose:

Quick Mode MUST be implemented as a mechanism to generate fresh keying material and negotiate non-ISAKMP security services.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	HOST-1 addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	HOST-1 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                         <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========      HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)       ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

The test sequence is following.

＊ IPsec transmission

```
 #   Initiator(TN)      Direction     Responder(NUT)
(1)IP_HDR; ESP*;
   ICMP(Echo request)   ========>                           <---Sequence Number = 1
(2)                    <========    IP_HDR;ESP*;ICMP     <---Sequence Number = 1
(3)IP_HDR; ESP*;                        (Echo reply)
   ICMP(Echo request)   ========>                           <---Sequence Number = 2
(4)                    <========      IP_HDR; ESP*; ICMP <---Sequence Number = 2
               Judgement (Check *1)     (Echo reply)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT).
   And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).
2. Receive the second message from NUT
   In the second message (2), responder(NUT) forward encrypted Echo reply from HOST-1(TN) to initiator(TN).
3. Send the third message from TN
   In the third message (3), initiator(TN) forward Echo request from HOST-2(TN) to responder(NUT).
   And NUT(SGW-1) forward decrypted Echo request to HOST-1(TN).
4. Receive the fourth message from NUT
   In the fourth message (4), responder(NUT) forward encrypted Echo reply from HOST-1(TN) to initiator(TN).

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly, In IPsec SA transmission, the second message's Sequence Number must be "1".
and the fourth message's Sequence Number must be "2".
And must conform to above Configuration.

References:

RFC2406 : 2. Encapsulating Security Payload Packet Format

7.4.41 Sequence Number Verification

Purpose:

Encapsulating Security Protocol Processing(Inbound Packet Processing)

- Sequence Number
  If the receiver has enabled the anti-replay service for this SA, the receive packet counter for the SA MUST be initialized to zero when the SA is established. For each received packet, the receiver MUST verify that the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packets received during the life of this SA. This SHOULD be the first ESP check applied to a packet after it has been matched to an SA, to speed rejection of duplicate packets.

Category:

End-Node : N/A
SGW : ADVANCED (This test is required for all SGW NUTs which support Receiver)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	HOST-1 addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	HOST-2 addr	HOST-1 addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                         <QUICK MODE>
 #    Initiator(TN)       Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>
(2)                       <========       HDR*, HASH(2), SA, Nr, IDci, IDcr;
(3)   HDR*, HASH(3)       ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3). HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.

The test sequence is following.

＊ IPsec transmission

```
 #   Initiator(TN)  Direction  Responder(NUT)
(1)IP_HDR; ESP*;
  ICMP(Echo request)========>              <------Sequence Number:1
(2)                            IP_HDR;ESP*;
                   <========ICMP(Echo reply)
(3)IP_HDR; ESP*;
   ICMP(Echo request)========>             <------Sequence Number:1(invalid)
               Judgement (Check *1)        <------Must not foward to HOST-1(TN)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) forward Echo request (Sequence Number:1) from HOST-2(TN) to HOST-1(TN) via responder(NUT).
2. Receive the second message from NUT
   In the second message (2), responder(NUT) forward Echo reply from HOST-1(TN) to HOST-2(TN) via initiator(TN).
3. Send the third message from TN
   In the third message (3), initiator(TN) forward Echo request (Sequence Number:1(invalid))from HOST-2(TN) to HOST-1(TN) via responder(NUT)

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first to the third message must be exchanged correctly,
In IPsec SA transmission, the third message must not be accepted.
And must not be fowarded to HOST-1(TN).

References:

RFC2406 : 3.4.3 Sequence Number Verification

7.4.42 Processing invalid ISAKMP Payload Length

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
  Length field = 0(invalid value)
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 # Initiator(TN)    Direction   Responder(NUT)
(1) HDR*, HASH(1),
   SA,Ni,IDci,IDcr; =======>                  <-----Length field
                                                  (ISAKMP header):0(invalid)
(2-A)             X <========HDR*,HASH(2),SA,Nr <-----Must not transmit
                              IDci, IDcr;
                                or
(2-B)               <========HDR*,HASH(1),N/D;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC 2408 : 5.1 General Message Processing

7.4.43 Processing invalid Initiator Cookie field

Purpose:

Verify the Initiator and Responder "cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
    Initiator Cookie field : 0 (not same Initiator cookie in Phase I)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)    Direction   Responder(NUT)
(1) HDR*, HASH(1),
    SA, Ni,IDci, IDcr;========>                <-----Initiator Cookie field
                                                              : 0 (invalid)
(2-A)              X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                 IDci, IDcr;
                                    or
(2-B)                <========   HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not returned (* or INVALID-COOKIE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.4.44 Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
    Next Payload field = 127(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 # Initiator(TN)    Direction    Responder(NUT)
(1)HDR*,HASH(1),
   SA,Ni,IDci,IDcr; ========>                    <-----Next Payload field
                                                  (ISAKMP Header):127(invalid)
(2-A)              X <======== HDR*,HASH(2),SA,Nr<-----Must not transmit
                                 IDci,IDcr;
                                   or
(2-B)                <======== HDR*,HASH(1),N/D;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal itconsiders adequate to protect traffic for the given situation. TheSecurity Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.4.45 Processing invalid Major Version field (major 15, minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR- VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
    Major Version 15 (invalid value)
    Minor Version 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

* PHASE II

```
                       <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni, IDci, IDcr; ========>                      <-----Major Version : 15
                                                                    (invalid)
(2-A)                X <========  HDR*, HASH(2), SA, Nr <-----Must not transmit
                                      IDci, IDcr;
                                         or
(2-B)                  <========   HDR*, HASH(1), N/D;
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message must not be returned(2-A) (* or INVALID-MAJOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format

7.4.46 Processing invalid Minor Version field (major 1, minor 15)

Purpose:

- Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:
  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.
  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
  This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Initiator,In Phase II)
    Major Version 1 (invalid value)
    Minor Version 15
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
* PHASE II
                          <QUICK MODE>
 # Initiator(TN)    Direction       Responder(NUT)
(1)HDR*, HASH(1),
  SA,Ni,IDci,IDcr; ========>                  <-----Miner Version:15(invalid)
(2-A)          X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                 IDci, IDcr;
                                    or
(2-B)            <========HDR*,HASH(1),N/D;
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I, messages must be exchanged correctly.
In Phase II, the first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MINOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

7.4.47 Processing invalid Exchange Type field

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
    Exchange Type field = 31(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                      <QUICK MODE>

 #    Initiator(TN)      Direction    Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                        <-----Exchange Type field
                                                                        :31(invalid)
(2-A)                  X <========   HDR*, HASH(2), SA, Nr <-----Must not transmit
                                     IDci, IDcr;
                                         or
(2-B)                    <========   HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.4.48 Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate systemaudit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ ISAKMP Header Format(HOST-2:Initiator, In Phase II)
  Flags field = |1|1|1|1|1|0|0|1|(invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 # Initiator(TN)    Direction     Responder(NUT)
(1)HDR*,HASH(1),
   SA,Ni,IDci,IDcr; ========>                   <-----Flags field :
                                                    |1|1|1|1|1|0|0|1|(invalid)
(2-A)             X <======== HDR*,HASH(2),SA,Nr<-----Must not transmit
                                  IDci, IDcr;
                                     or
(2-B)               <======== HDR*,HASH(1),N/D;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) is not returned (* or INVALID-FLAGS message(2-B) is returned).*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.4.49 Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values.
If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ISAKMP Header Format(HOST-2:Initiator, In Phase II)
    In PHASE II of TEST PROCEDURE, Message ID field of the third message is set to 0(not same the first message's Message ID).
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
#   Initiator(TN)     Direction  Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr;========>
(2)                     <======== HDR*, HASH(2), SA, Nr
                                  IDci, IDcr;
(3)  HDR*, HASH(3)     ========>                  <-----Message ID:0(invalid)
(4)                    <======== HDR*, HASH(1), N/D <-----must not establish
                   Judgement (Check *1)                              IPsec SA
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.
3. Send the third message from TN
   In the third (3) message, the initiator send HASH(3).
   HASH(3)-- for liveliness-- is the prf over the value zero represented as a single octet, followed by a concatenation of the message id and the two nonces-- the initiator's followed by the responder's-- minus the payload header.
4. Receive the fourth message from NUT
   In the fourth message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

＊ IPsec transmission

```
 #   Initiator(TN)     Direction     Responder(NUT)
(1)IP_HDR; ESP*;
   ICMP(Echo request)=======>
(2)                X <=======IP_HDR;ESP*;ICMP(Echo reply) <---must not transmit
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), initiator(TN) send Echo request to responder (NUT) with IPsec SA.

2. Receive the second message from NUT
   In the second message (2), responder(NUT) send Echo reply to initiator (TN) with IPsec SA.(In this case, responder must not transmit Echo reply)

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first and the second message must be exchanged correctly.
the third message must not be accepted. And the fourth message is not returned or INVALID-MESSAGE-ID message is returned(must not establish IPsec SA).
In IPsec transmission, the first message must not be accepted.
The second message must not be returned.

References:

RFC2408 : 5.2 ISAKMP Header Processing

7.4.50 Processing invalid Next Payload field

Purpose:

If the Next Payload field validation fails, the message is discarded.

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - SA Payload Format(HOST-2:Initiator, In Phase II)
    Next Payload field : 127(invalid value)
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  * PHASE Ⅰ
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 # Initiator(TN)  Direction Responder(NUT)
(1)HDR*, HASH(1),
   SA,Ni,IDci,IDcr;========>             <-----Next Payload field:127(invalid)
(2-A)           X <======== HDR*,HASH(2),SA,Nr <-----Must not transmit
                              IDci, IDcr;
                                or
(2-B)             <======== HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.
   In this test, INVALID-PAYLOAD-TYPE Notify message is send.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase Ⅰ, messages must be exchanged correctly.
In Phase Ⅱ, the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
           5.3 Generic Payload Header Processing

7.4.51 Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator, In Phase II)
    RESERVED field : 1(set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(TN)      Direction     Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                     <-----RESERVED field : 1
                                                                     (invalid)
(2-A)                  X <========  HDR*, HASH(2), SA, Nr <-----Must not transmit
                                         IDci, IDcr;
                                             or
(2-B)                   <========  HDR*, HASH(1), N/D;
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.3 Generic Payload Header Processing

7.4.52 Processing invalid Hash Payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Initiator, In Phase II)
    Hash Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 # Initiator(TN)     Direction  Responder(NUT)
(1)HDR*, HASH(1),
   SA,Ni,IDci,IDcr; ========>                <-----Hash Data field:not include
                                                   this field(invalid)
(2-A)          X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                 IDci,IDcr;
                                     or
(2-B)            <========HDR*,HASH(1),N/D;
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-HASH-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.4.53 Processing invalid Hash Data field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  ✧ Hash Payload Format(HOST-2:Initiator,In Phase II)
  Hash Data field : 0 (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)  Direction  Responder(NUT)
(1) HDR*, HASH(1),
   SA, Ni,IDci, IDcr; ========>              <-----Hash Data field : 0(invalid)
(2-A)            X <======== HDR*, HASH(2), SA, Nr <-----Must not transmit
                             IDci, IDcr;
                                 or
(2-B)             <========  HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or AUTHENTICATION-FAILED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.11 Hash Payload Processing

7.4.54 Processing invalid Next Payload field

Purpose:

- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ SA Payload Format(HOST-2:Initiator, In Phase II)
  Next Payload field : 2(Proposal Payload, invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                    <QUICK MODE>
#   Initiator(TN) Direction   Responder(NUT)
(1)HDR*,HASH(1),
  SA,Ni,IDci,IDcr;========>              <-----Next Payload field:2(invalid)
(2-A)           X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                              IDci, IDcr;
                                 or
(2-B)             <========HDR*,HASH(1),N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.
   In this test, INVALID-PAYLOAD-TYPE Notify message is send.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
5.3 Generic Payload Header Processing

7.4.55 Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported. If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator, In Phase II)
    Domain of Interpretation field : 0xffffffff(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #    Initiator(TN)     Direction   Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                  <-----DOI field:0xffffffff
                                                                   (invalid)
(2-A)            X <======== HDR*, HASH(2), SA, Nr <-----Must not transmit
                             IDci, IDcr;
                                or
(2-B)              <======== HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or DOI-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.56 Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator, In Phase II)
    Situation field : 0x80000000(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>                    <-----Situation field:
                                                                0x80000000
(2-A)               X <========  HDR*, HASH(2), SA, Nr <-----Must not transmit
                                        IDci, IDcr;
                                         or
(2-B)                 <========  HDR*, HASH(1), N/D;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not accepted.
And the second message(2-A) must not be returned (* or SITUATION-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.57 Processing invalid proposal(ESP Authentication)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	61439	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                      <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                          <-----invalid proposal
(2-A)                X <========    HDR*, HASH(2), SA, Nr <-----Must not transmit
                                     IDci, IDcr;
                                          or
(2-B)                  <========    HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned
(* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.58 Processing invalid proposal(Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal,Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	32767	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1), SA,
     Ni, KE ,IDci, IDcr;========>                     <-----invalid proposal
(2-A)                X <========HDR*,HASH(2),SA,Nr,KE <-----Must not transmit
                               IDci, IDcr;
                                  or
(2-B)                  <======== HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.59 Processing invalid proposal(Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ SA attribute(HOST-2:Initiator, In Phase II)
    Life Type : 65000(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>                        <-----invalid proposal
(2-A)                 X <======== HDR*, HASH(2), SA, Nr  <-----Must not transmit
                                  IDci, IDcr;
                                         or
(2-B)                  <======== HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.60 Processing invalid proposal(Encapsulation Mode)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	61439	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                     <QUICK MODE>
 #   Initiator(TN)      Direction      Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr; ========>                     <-----invalid proposal
(2-A)               X <========  HDR*, HASH(2), SA, Nr <-----Must not transmit
                                     IDci, IDcr;
                                        or
(2-B)                 <========  HDR*, HASH(1), N/D;
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

7.4.61 Processing invalid Protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Proposal Payload Format(HOST-2:Initiator, In Phase II)
  Protocol-ID field : 248(invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	**Src**	**Dest**	**Phase II**							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
# Initiator(TN)   Direction  Responder(NUT)
(1)HDR*,HASH(1),
  SA,Ni,IDci,IDcr;========>                  <-----Protocol-ID field :
                                                        248(invalid)
(2-A)          X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                IDci, IDcr;
                                             or
(2-B)             <======== HDR*, HASH(1), N/D;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-PROTOCOL-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.4.62 Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Initiator, In Phase II)
    SPI field : SPI value is set as 0.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                           <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni, IDci, IDcr; ========>                  <-----SPI field : 0(invalid)
(2-A)              X <======== HDR*, HASH(2), SA, Nr <-----Must not transmit
                                  IDci, IDcr;
                                      or
(2-B)                <======== HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-SPI message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.4.63 Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Initiator, In Phase II)
    Number of Transforms field : 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #    Initiator(TN)      Direction   Responder(NUT)
(1)   HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                        <-----Number of Transforms
                                                                    field:0(invalid)
(2-A)                  X <========HDR*,HASH(2),SA,Nr <-----Must not transmit
                                   IDci, IDcr;
                                       or
(2-B)                    <======== HDR*,HASH(1),N/D;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

7.4.64 Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Initiator, In Phase II)
    Transform-ID field : 248(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	248	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1),
      SA, Ni,IDci, IDcr; ========>                    <-----Transform-ID field:
                                                                  248(invalid)
(2-A)                 X <========HDR*,HASH(2),SA,Nr <-----Must not transmit
                                  IDci, IDcr;
                                     or
(2-B)                   <======== HDR*,HASH(1),N/D;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload. IDci and IDcr is identification information.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not accepted.
And the second message(2-A) must not returned (*or INVALID-TRANSFORM-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.4.65 Processing invalid Transform Payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Initiator, In Phase II)
    SA Attributes field : not set(see below)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP					Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- **Pre-Sequence**
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)       Direction    Responder(NUT)
(1)  HDR*, HASH(1),
     SA, Ni,IDci, IDcr;   ========>                   <-----invalid SA Attributes
(2-A)                  X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                  IDci, IDcr;
                                      or
(2-B)                    <========HDR*,HASH(1),N/D;
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not accepted.
And the second message must not be returned(2-A) (* or BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(2-B) is returned.
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

7.4.66 Attribute Parsing Requirement (conflicting attributes)

Purpose:

If conflicting attributes are detected, an ATTRIBUTES-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA		8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                         <QUICK MODE>
 # Initiator(TN)      Direction      Responder(NUT)
(1) HDR*, HASH(1),
    SA,Ni,IDci,IDcr; ========>                  <------ conflicting attributes
                                                                     (invalid)
(2-A)               X <========HDR*,HASH(2),SA,Nr<-----Must not transmit
                                     IDci, IDcr;
                                       or
(2-B)                 <======== HDR; N/D
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
The second message must not be returned (or ATTRIBUTES-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2407 : 4.5.2 Attribute Parsing Requirement (Lifetime)

7.4.67 Multiple Proposal and Transform Payloads (reject proposal)

Purpose:

The receiving entity MUST select a single transform for each protocol in a proposal or reject the entire proposal.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
  For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II									
			Prop #	Proto ID	Trans #	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr		PROTO_IPSEC_ESP		ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	1	PROTO_IPSEC_AH	2	247	Tunnel	61438	8 Hour	Net-v addr	Net-z addr	any
					2	248	Tunnel	61439	8 Hour			
			1	PROTO_IPSEC_ESP	2	247	Tunnel	61438	8 Hour			
					2	248	Tunnel	61439	8 Hour			

  For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                       <QUICK MODE>
 #    Initiator(TN)      Direction       Responder(NUT)
(1)   HDR*, HASH(1),
    SA,Ni,IDci,IDcr; ========>                        <-----invalid proposal
(2)                X <======== HDR*,HASH(2),SA,Nr   <-----Must not transmit
                                      IDci, IDcr;
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce. HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message is not accepted.
And the second message(2) must not be returned.

References:

RFC2408 : 4.2 Security Association Establishment

7.4.68 Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - ✧ Key Exchange Payload Format(HOST-2:Initiator, In Phase II)
    Key Exchange Data field : 0(1byte)(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II								
			Proto ID	Trans ID	Mode	Auth Alg	DH Group	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	2	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(TN)     Direction   Responder(NUT)
(1) HDR*, HASH(1), SA,
    Ni,KE ,IDci,IDcr;========>                   <-----Key Exchange Data
                                                     field : 0(1byte)(invalid)
(2-A)            X <========HDR*,HASH(2),SA,Nr,KE<-----Must not transmit
                                 IDci, IDcr;
                                     or
(2-B)               <========  HDR*, HASH(1), N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.KE is keying material used to arrive at a common shared secret. IDci and IDcr is identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted.
And the second message(2-A) must not be returned (* or INVALID-KEY-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.7 Key Exchange Payload Processing

7.4.69 Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- **Configuration**
  - ✧ Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::
  - ✧ Identification Payload Format(IDcr, In Phase II)
    (NUT:SGW-1) Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    (TN:SGW-2) Identification Type field : 248(invalid value)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	Trans ID	Mode	Auth Alg	PH2 Lt	IDci	IDcr	Upper
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence
  * PHASE I
  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)     Direction   Responder(NUT)
(1)HDR*,HASH(1),
   SA,Ni,IDci,IDcr;========>                  <----ID Type field:248(invalid)
(2-A)           X <========HDR*,HASH(2),SA,Nr,
                          IDci, IDcr;         <----Must not transmit
                              or
(2-B)             <========HDR*, HASH(1),N/D;
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

IIn Phase I , messages must be exchanged correctly.
In Phase II , the first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-ID-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.8 Identification Payload Processing

7.4.70 Invalid Identification Payload

Purpose:

If the client identities are not acceptable to the Quick Mode responder (due to policy or other reasons), a Notify payload with Notify Message Type INVALID-ID-INFORMATION (18) SHOULD be sent.

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs)

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for SGW vs. SGW (Responder Test)".

- Configuration
  - Identification Payload Format(IDci, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    (NUT:SGW-1) Identification Data field :
    3ffe:501:ffff:104::,ffff:ffff:ffff:ffff::
    (TN:SGW-2) Identification Data field : ::(invalid value)
  - Identification Payload Format(IDcr, In Phase II)
    Identification Type field : 6(ID_IPV6_ADDR_SUBNET)
    Protocol ID field : 0(any)
    Port field : 0(any)
    Identification Data field : 3ffe:501:ffff:100::,ffff:ffff:ffff:ffff::
  - Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 Configuration, refer "Table 1. Phase-1 Common Configuration" in Chapter "Common Configuration".
    For Phase-2 configuration, use following parameter.

Machine	Src	Dest	Phase II							
			Proto ID	**Trans ID**	**Mode**	**Auth Alg**	**PH2 Lt**	**IDci**	**IDcr**	**Upper**
SGW-1	SGW-1 addr	SGW-2 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	Net-v addr	Net-z addr	any
SGW-2	SGW-2 addr	SGW-1 addr	PROTO_IPSEC_ESP	ESP_3DES	Tunnel	HMAC-SHA	8 Hour	::	Net-z addr	any

For abbr., refer "Configuration Table" part in Chapter "Terminology".

- Pre-Sequence

  * PHASE I

  For Phase-1 Sequence, refer "4.2Phase-1 Sequence (Responder Test)"

Procedure:

The test sequence is following.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)     Direction   Responder(NUT)
(1)HDR*,HASH(1),
  SA,Ni,IDci,IDcr;========>                    <-----ID data field : ::(invalid)
(2-A)           X <========HDR*,HASH(2),SA,Nr,<-----Must not transmit
                                IDci, IDcr;
                                  or
(2-B)             <======== HDR*,HASH(1),N/D
                Judgement (Check *1)
```

1. Send the first message from TN

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness. IDci and IDcr is identification information.
2. Receive the second message from NUT

   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

In Phase I , messages must be exchanged correctly.
In Phase II , the first message is not accepted. The second message(2-A) must not be returned (* or INVALID-ID-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2409 : 5.5 Phase 2 - Quick Mode