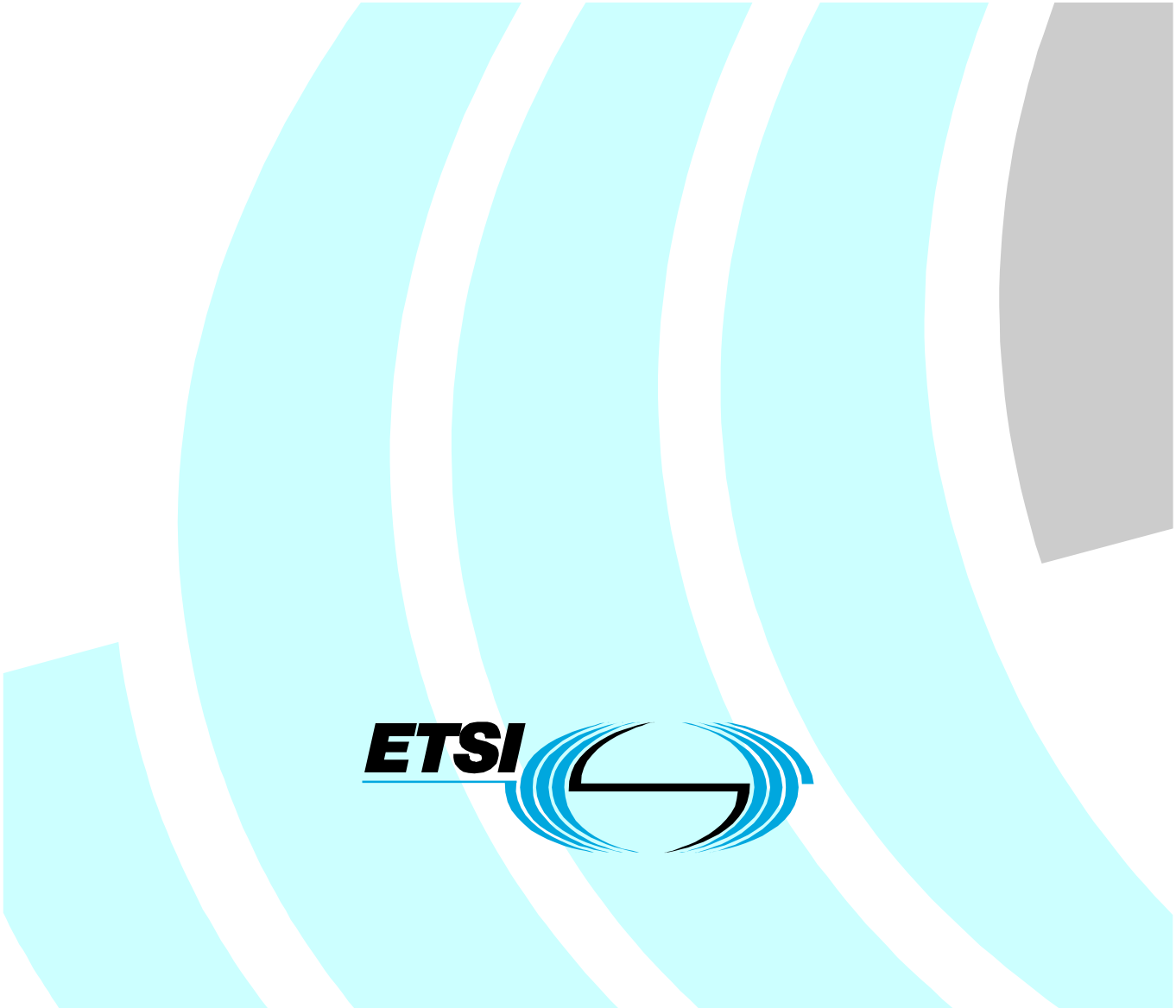
ETSI TS 102 597 V1.1.1 (2007-05)

Technical Specification

Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Interoperability Test Suite



Reference
DTS/MTS-IPT-012-IPv6-SecITS

Keywords
interoperability, IP, IPv6, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Introduction

IPv6 is the next generation Internet. It gives vastly increased address space and true end-to-end communication. It has improved security and mobility features and allows "plug-and-play" connection to the network. The complexity of implementing IPv6 technology and the relative openness of IETF standards means that wide-ranging and effective testing of IPv6 products will be one of the key factors in ensuring the deployment, interoperability, security and reliability of the IPv6 infrastructure.

The present document specifies interoperability tests for IPv6 Security. The test suite results from and analysis of RFC 4301 [3], RFC 4302 [4], RFC 4303 [5], RFC 4305 [6] and RFC 4306 [7], the extraction of the requirements contained in these documents, and a selection of the requirements which could be tested by interoperability means.

The methodology and framework used to analyse the RFCs, to extract the requirements, write the Test Purposes, and the test descriptions is described in TS 102 351 [1].The reader is strongly encouraged to read TS 102 351 [1] in order to make the best usage of the present document.

1 Scope

The present document specifies the interoperability Test Descriptions (TDs) with integrated Test Purposes (TPs) for the selected IPv6 Security standards. The TDs are presented in the tabular form specified in TS 102 424 [8] and the TPs are defined using the TPLan notation also described in ES 202 553 (see bibliography).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

[1] ETSI TS 102 351: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); IPv6 Testing: Methodology and Framework".

[2] ETSI TS 102 558 "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Requirements Catalogue".

[3] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[4] IETF RFC 4302: "IP Authentication Header".

[5] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[6] IETF RFC 4305: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[7] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[8] ETSI TS 102 424: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements of the NGN network to support Emergency Communication from Citizen to Authority".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EUT	Equipment Under Test
MTU	Maximum Transmission Unit
QE	Qualified Equipment
TP	Test Purpose
TD	Test Description
TPLan	Test Purpose Language
TSS	Test Suite Structure

4 IPv6 Security Interoperability Test Specification

4.1 Test Descriptions

The IPv6 Security Interoperability Test Descriptions (TDs) defined in the following clauses are derived from the Test Purposes (TPs) specified in Annex .

Test Description presentation and concepts are explained in TS 102 351 [1].

Requirements referred to within the Test Description (example: RQ_001_1016) are all contained in TS 102 558 [2], the IPv6 Security "Requirements catalogue".

4.1.1 Index of test grouping

In the present document, tests have been grouped according to the original RFC from which they were extracted.

NOTE: Test Descriptions covering requirements coming from more than one group are repeated in the relevant groups.

4.2 Test Descriptions

Group 1: RFC 4301 - Internet Security Architecture

Test Description			
Identifier:	TD_SEC_1004_01	**Test Purpose:**	TP_SEC_1004_01
Summary:	'Support of ESP'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1004		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP'
         and QE1 configured 'to protect all traffic to/from EUT using ESP'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP to secure all communications to and from QE1 b. QE1 will use ESP to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:	.		

Test Description			
Identifier:	TD_SEC_1005_01	**Test Purpose:**	TP_SEC_1005_01
Summary:	'Support of AH'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1005		

```
with {     EUT configured 'to protect all traffic to/from QE1 using AH'
         and QE1 configured 'to protect all traffic to/from EUT using AH'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use the Authentication Header (AH) to secure all communications to and from QE1 b. QE1 will use the Authentication Header (AH) to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1020_01	**Test Purpose:**	TP_SEC_1020_01
Summary:	'IPsec Host support of ESP transport mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1020, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Transport Mode to secure all communications to and from QE1 b. QE1 will use ESP in Transport Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to establish a Security association with EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1020_02	**Test Purpose:**	TP_SEC_1020_02
Summary:	'IPsec Host support of AH transport mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1020, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE1 using AH
                          with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                          with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Transport Mode to secure all communications to and from QE1 b. QE1 will use AH in Transport Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1021_01	**Test Purpose:**	TP_SEC_1021_01
Summary:	'IPsec Host support of ESP tunnel mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1021, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
       }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Tunnel Mode to secure all communications to and from QE1 b. QE1 will use ESP in Tunnel Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1021_02	**Test Purpose:**	TP_SEC_1021_02
Summary:	'IPsec Host support of AH tunnel mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1021, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE1 using AH
                          with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                          with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Tunnel Mode to secure all communications to and from QE1 b. QE1 will use AH in Tunnel Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1022_01	**Test Purpose:**	TP_SEC_1022_01
Summary:	'IPsec Gateway support of ESP tunnel mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1022, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                          with the tunnel mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Tunnel Mode to secure all communications to and from QE4 b. QE4 will use ESP in Tunnel Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1022_02	**Test Purpose:**	TP_SEC_1022_02
Summary:	'IPsec Gateway support of AH tunnel mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1022, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE4 using AH
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                          with the tunnel mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Tunnel Mode to secure all communications to and from QE4 b. QE4 will use AH in Tunnel Mode to secure all communications to and from the EUT c. QE1 will only accept secure communication from QE2 d. QE2 will only accept secure communication from QE1 Security Association established from QE2 to QE1 Security Association established from QE1 to QE1

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1023_01	**Test Purpose:**	TP_SEC_1023_01
Summary:	'IPsec Gateway Support of ESP transport mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1023, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                          with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                          with the transport mode'
     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Transport Mode to secure all communications to and from QE4 b. QE4 will use ESP in Transport Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1023_02	**Test Purpose:**	TP_SEC_1023_02
Summary:	'IPsec Gateway Support of AH transport mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1023, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE4 using AH
                          with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                          with the transport mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Transport Mode to secure all communications to and from QE4 b. QE4 will use AH in Transport Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Group 2: RFC 4306 - Internet Key Exchange protocol (IKEv2)

Group 2.1: Information Exchanges

Test Description			
Identifier:	TD_SEC_6010_01	**Test Purpose:**	TP_SEC_6010_01
Summary:	'An IKE implementation should close a Security Associations upon receipt of an INFORMATION request with a Delete payload identifying that particular SA'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6010		

```
with {     EUT configured 'to accept traffic from QE1 only if secured'
       and QE1 'having successfully established multiple Child_SAs with EUT'
     }
ensure that {
  when  { EUT receives an INFORMATION_Request from QE1
              containing a DELETE_payload
              for a security_association between QE1 and the EUT}
  then  { QE1 and EUT are unable to communicate securely
                    using that security_association}
            }
```

Pre-test conditions:	Security Policy defined such that: a. QE1 will accept only secure communications from the EUT b. The EUT will accept both secure and non-secure communications from QE1 c. QE1 will use ESP in Tunnel Mode for all ICMP6 transmissions to the EUT d. QE1 will use ESP in Transport Mode for all UDP transmissions to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Preamble: Cause the EUT to send an Echo Request to QE1 (establishing an IKE_SA with an ESP Tunnel Mode Child_SA)		
2	Preamble: Check: Does the EUT receive an Echo Reply from QE1?	Yes	No
3	Preamble: Cause the EUT to send Tracepath to QE1 (establishing an additional Child_SA using ESP in Tunnel Mode)		
4	Preamble: Check: Does the EUT receive a Tracepath response indicating that QE1 was reached?	Yes	No
5	Cause QE1 to delete the ESP Tunnel Mode CHILD_SA to the EUT		
6	Cause the EUT to send an Echo Request to QE1		
7	Check: Does the EUT receive an Echo Reply from QE1?	No	Yes
8	Cause the EUT to send Tracepath to QE1		
9	Check: Does the EUT receive a Tracepath response indicating that QE1 was reached?	Yes	No
Observations:	Untestable by IOP means		

Test Description			
Identifier:	TD_SEC_6011_01	**Test Purpose:**	TP_SEC_6011_01
Summary:	'An IKE implementation should delete Child_SAs when the associated IKE_SA is deleted'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6011		

```
with {      EUT configured 'to accept traffic only if secured'
        and QE1 'having successfully established a single IKE SA with EUT'
        and QE1 'having successfully established some CHILD SAs with EUT'
     }
ensure that {
  when  { EUT receives an INFORMATION_Request from the EUT
             containing a DELETE_payload
             for the IKE_SA between QE1 and the EUT}
  then  { QE1 and EUT are unable to communicate securely }
            }
```

Pre-test conditions:	Security Policy defined such that: a. QE1 will accept only secure communications from the EUT b. The EUT will accept both secure and non-secure communications from QE1		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause the EUT to send an Echo Request to QE1		
2	Check: Does the EUT receive an Echo Reply from QE1?	Yes	no
3	Cause QE1 to delete the IKE_SA to the EUT		
4	Cause the EUT to send an Echo Request to QE1		
5	Check: Does the EUT receive an Echo Reply from QE1?	No	Yes
Observations:	Untestable by IOP means		

Test Description			
Identifier:	TD_SEC_6041_01	**Test Purpose:**	TP_SEC_6041_01
Summary:	"An IKE endpoint should accept and process requests while it is waiting for responses to its own requests"		
Roles:	Host, Ipsec_host	**Configuration:**	CF_SEC_04
References:	RQ_002_6041, RQ_002_6041		

```
with {      EUT configured 'only to communicate securely with QE1'
        and EUT configured 'only to communicate securely with QE6'
     }
ensure that {
  when {    EUT sends an IKE_SA_INIT_Request to QE6
        and QE6 is unable to send an immediate IKE_SA_INIT_Response to the EUT }
  then  { EUT and QE1 are able to communicate securely
          before the EUT receives an IKE_SA_INIT_Response from QE6 }
            }
```

Pre-test conditions:	Not testable by Interoperability means. How is it possible to block the IKE_SA_INIT_Response coming from QE6? We cannot disconnect it because NS will not work - so IKE_SA_INIT_Request will not be sent		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
Observations:	Untestable by IOP means		

Group 2.2: Message Length

Test Description			
Identifier:	TD_SEC_6024_01	**Test Purpose:**	TP_SEC_6024_01
Summary:	'An IKE implementation should be able to send IKE messages that are up to 1 280 bytes long'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6024		

```
with {      EUT configured 'to use certificate authentication with
                           certificates leading to 1 280 bytes long messages'
        and QE1 configured 'to support certificate authentication'
    }
ensure that {
  when  { EUT  sends an IKE_SA_INIT_Request to QE1 }
  then  { EUT and QE1 are able to communicate securely }
          }
```

Pre-test conditions:	Security policy defined such that: a. The EUT will accept only secure communication from QE1 b. QE1 will accept only secure communicaation from the EUT c. The EUT will use certificate authentication with certificates leading to 1 280 bytes long messages d. QE1 will support certificate authentication		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause EUT to send an Echo Request to QE1, which leads to Security Association establishment		
2	Check: Does EUT receive an Echo Reply?	Yes	No
Observations:	.		

Test Description			
Identifier:	TD_SEC_6025_01	**Test Purpose:**	TP_SEC_6025_01
Summary:	'An IKE implementation should be able to receive and process IKE messages that are up to 1 280 bytes long'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6025		

```
with {      EUT configured 'to support certificate authentication'
        and QE1 configured 'to use certificate authentication with
                            certificates leading to 1 280 bytes long messages'
    }
ensure that {
  when  { QE1 sends an IKE_SA_INIT_Request to the EUT }
  then  { EUT and QE1 are able to communicate securely }
          }
```

Pre-test conditions:	Security policy defined such that: a. the EUT will accept only secure communication from QE1 b. QE1 will accept only secure communicaation from the EUT c. QE1 will use certificate authentication with certificates leading to 1 280 bytes long messages d. the EUT will support certificate authentication		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT, which leads to Security Association establishment		
2	Check: Does QE1 receive an Echo Reply?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_6026_01	**Test Purpose:**	TP_SEC_6026_01
Summary:	'An IKE implementation should be able to send IKE messages that are up to 3 000 bytes long'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6026		

```
with {      EUT configured 'to use certificate authentication with
                           certificates leading to 3 000 bytes long messages'
        and QE1 configured 'to support certificate authentication'
    }
ensure that {
  when  { EUT sends an IKE_SA_INIT_Request to QE1 }
  then  { EUT and QE1 are able to communicate securely }
          }
```

Pre-test conditions:	Security policy defined such that: a. The EUT will accept only secure communication from QE1 b. QE1 will accept only secure communicaation from the EUT c. The EUT will use certificate authentication with certificates leading to 3 000 bytes long messages d. QE1 will support certificate authentication		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause EUT to send an Echo Request to QE1, which leads to Security Association establishment		
2	Check: Does EUT receive an Echo Reply?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_6027_01	**Test Purpose:**	TP_SEC_6027_01
Summary:	'An IKE implementation should be able to receive and process IKE messages that are up to 3 000 bytes long'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_6027		

```
with {      EUT configured 'to support certificate authentication'
        and QE1 configured 'to use certificate authentication with
                           certificates leading to 3 000 bytes long messages'
    }
ensure that {
  when  { QE1 sends an IKE_SA_INIT_Request to the EUT }
  then  { EUT and QE1 are able to communicate securely }
          }
```

Pre-test conditions:	Security policy defined such that: a. The EUT will accept only secure communication from QE1 b. QE1 will accept only secure communicaation from the EUT c. QE1 will use certificate authentication with certificates leading to 3 000 bytes long messages d. The EUT will support certificate authentication		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT, which leads to Security Association establishment		
2	Check: Does QE1 receive an Echo Reply?	Yes	No
Observations:			

Group 2.3: Security Parameter Negotiation

Group 2.3.1: Algorithm Negotiation

Test Description			
Identifier:	TD_SEC_6372_01	**Test Purpose:**	TP_SEC_6372_01
Summary:	'An IKE implementation selects a single security proposal from the set of proposals received from the other endpoint in a Security Association'		
Roles:	Host, Host	**Configuration:**	CF_SEC_01
References:	RQ_002_6372, RQ_002_6372		

```
with { EUT configured 'to support at least one of the security proposals
                       available to QE1'
     }
ensure that {
  when  { the EUT receives an IKE_SA_INIT_request from QE1
                  containing at least 1 proposal
      and the EUT is able to support at least 1 proposal }
  then  { the EUT establishes a Security_Association to QE1
                          using 1 proposal }
              }
```

Pre-test conditions:	Untestable by IOP means		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
Observations:			

Test Description			
Identifier:	TD_SEC_6372_02	**Test Purpose:**	TP_SEC_6372_02
Summary:	'An IKE implementation is unable to select a security proposal from the set of proposals received from the other endpoint in a Security Association'		
Roles:	Host, Host	**Configuration:**	CF_SEC_01
References:	RQ_002_6372, RQ_002_6372		

```
with { EUT configured 'so that it does not support any of the security
                       proposals available to QE1'
     }
ensure that {
  when  { the EUT receives an IKE_SA_INIT_request from QE1
                  containing at least 1 proposal
      and the EUT is unable to support even 1 proposal }
  then  { the EUT rejects the IKE_SA_INIT_request
                  indicating NO_PROPOSAL_CHOSEN }
              }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communications from QE1 b. QE1 will accept only secure communications from the EUT c. The EUT will not support any of the security proposals available to QE1		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo request to EUT		
2	Check: Does QE1 receive an Echo Reply?	No	Yes
Observations:			

Group 2.3.2: Security Association Lifetime

Test Description			
Identifier:	TD_SEC_6096_01	**Test Purpose:**	TP_SEC_6096_01
Summary:	'A Security Association is replaced if there is a continuing demand after the lifetime of the SA has expired'		
Roles:	Host	**Configuration:**	CF_SEC_01
References:	RQ_002_6096		

```
with  {  a Security_Association established between the EUT and QE1
       and 'regular secure traffic flowing between the EUT and QE1'
      }
ensure that {
  when  { the EUT detects the expiry of the lifetime of the Security_Association
          between the EUT and QE1 }
  then  { the EUT and QE1 are able to communicate securely }
          }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communication from QE1 b. QE1 will accept only secure communication from the EUT c. Security Associations established by the EUT will have a lifetime of 20 s		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Preamble: Cause the EUT to send an Echo Request to QE1		
2	Preamble: Check: Does the EUT receive an Echo Reply from QE1?	Yes	No
3	Cause the EUT to send repeated Echo Requests to QE1 for 30 seconds		
4	Cause the EUT to send an Echo Request to QE1		
5	Check: Does the EUT receive an Echo Reply from QE1?	Yes	No
Observations:	Step 1 leads to SA establishment between EUT and QE1 Untestable By IOP means		

Group 2.3.3: Traffic Selector Negotiation

Test Description			
Identifier:	TD_SEC_6121_01	**Test Purpose:**	TP_SEC_6121_01
Summary:	'A Security Association is created by an IKE endpoint if data is received from a host that is recognized as protected'		
Roles:	Host	**Configuration:**	CF_SEC_01
References:	RQ_002_6121		

```
with  {    EUT configured 'with no Security Association to QE1'
       and EUT configured ' to recognize QE1 as protected (in its SPD)'
      }
ensure that {
  when { the EUT receives a packet from QE1 }
  then { a Security_Association is established between the EUT and QE1 }
         }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communication from QE1 b. QE1 will accept both secure and non-secure communication from the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
3	Cause the EUT to send an Echo Request to QE1		
4	Check: Does the EUT receive an Echo Reply from QE1?	Yes	No
Observations:			

Group 2.4: NAT Traversal

Test Description			
Identifier:	TD_SEC_6206_01	**Test Purpose:**	TP_SEC_6206_01
Summary:	'An IKE endpoint accepts messages with any UDP Source port'		
Roles:	Host, Host	**Configuration:**	CF_SEC_02
References:	RQ_002_6206, RQ_002_6131, RQ_002_6206, RQ_002_6212		

```
with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
    and QE3 configured 'to translate UDP Source Port numbers for NAT traversal'
    and QE4 configured 'to translate UDP Source Port numbers for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
        }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communications from QE2 b. QE2 will accept only secure communications from the EUT QE3 is configured to translate UDP Source Port numbers for NAT traversal QE4 is configured to translate UDP Source Port numbers for NAT traversal		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE2 to send Traceroute to the EUT		
2	Check: Does QE2 receive a Traceroute response indicating that the EUT was reached?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_6212_01	**Test Purpose:**	TP_SEC_6212_01
Summary:	'An IKE endpoint sets UDP Destination Port number in IKE responses to the UDP Source Port number from the associated IKE request'		
Roles:	Host	**Configuration:**	CF_SEC_02
References:	RQ_002_6212		

```
with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
    and QE3 configured 'to translate UDP Source Port numbers for NAT traversal'
    and QE4 configured 'to translate UDP Source Port numbers for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
        }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communications from QE2 b. QE2 will accept only secure communications from the EUT QE3 is configured to translate UDP Source Port numbers for NAT traversal QE4 is configured to translate UDP Source Port numbers for NAT traversal		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE2 to send a Traceroutet to EUT (which leads to the establishment of a Security Association between QE2 and EUT)		
2	Check: Does QE2 receive a Traceroute response indicating that the EUT was reached?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_6213_01	**Test Purpose:**	TP_SEC_6213_01
Summary:	'An IKE endpoint sets IPv6 Destination Address in IKE responses to the IPv6 Source Address from the associated IKE request'		
Roles:	Host	**Configuration:**	CF_SEC_02
References:	RQ_002_6213		

```
with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
    and QE3 configured 'to translate IPv6 Source Addresses for NAT traversal'
    and QE4 configured 'to translate IPv6 Source Addresses for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
        }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communications from QE2 b. QE2 will accept only secure communications from the EUT QE3 is configured to translate IPv6 Source Addresses for NAT traversal QE4 is configured to translate IPv6 Source Addresses for NAT traversal		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE2 to send an Echo Request to EUT (which leads to the establishment of a Security Association between QE2 and EUT)		
2	Check: does QE2 receive an Echo Reply from EUT?	Yes	No
Observations:			

Group 2.5: Retransmission Timers

Test Description			
Identifier:	TD_SEC_6031_01	**Test Purpose:**	TP_SEC_6031_01
Summary:	'An IKE endpoint is able to identify and process a received response to any of its IKE request'		
Roles:	Host	**Configuration:**	CF_SEC_04
References:	RQ_002_6031		

```
with  {    EUT configured 'only to communicate securely with QE1'
       and EUT configured 'only to communicate securely with QE6'
       and QE6 configured 'only to communicate securely with EUT'
       and QE1 configured 'only to communicate securely with the EUT'
       and 'continual communication established between the EUT and QE6'
      }
ensure that {
  when { EUT establishes a Security_Association to QE1 }
  then { EUT and QE2 are able to communicate securely }
         }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure communications from QE1 b. The EUT will accept only secure communications from QE6 c. QE1 will accept only secure communications from the EUT d. QE6 will accept only secure communications from the EUT

Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Preamble: Cause QE6 to send unlimited, repeated Echo Requests to the EUT		
2	Cause EUT to send an Echo Request to QE1 (which leads to Security Association establishment)		
3	Check: does EUT receive an Echo Reply from QE1?	Yes	No
4	Postamble: Cause QE6 to cease sending Echo Requests to the EUT		
Observations:	Untestable by IOP		

Group 3: RFC 4303 - IP Encapsulating Security Protocol (ESP)

Test Description			
Identifier:	TD_SEC_1020_01	**Test Purpose:**	TP_SEC_1020_01
Summary:	'IPsec Host support of ESP transport mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1020, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Transport Mode to secure all communications to and from QE1 b. QE1 will use ESP in Transport Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to establish a Security association with EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1020_02	**Test Purpose:**	TP_SEC_1020_02
Summary:	'IPsec Host support of AH transport mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1020, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE1 using AH
                          with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                          with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Transport Mode to secure all communications to and from QE1 b. QE1 will use AH in Transport Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1023_01	**Test Purpose:**	TP_SEC_1023_01
Summary:	'IPsec Gateway Support of ESP transport mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1023, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                          with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                          with the transport mode'     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Transport Mode to secure all communications to and from QE4 b. QE4 will use ESP in Transport Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1023_02	**Test Purpose:**	TP_SEC_1023_02
Summary:	'IPsec Gateway Support of AH transport mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1023, RQ_002_3039		

```
with {     EUT configured 'to protect all traffic to/from QE4 using AH
                          with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                          with the transport mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Transport Mode to secure all communications to and from QE4 b. QE4 will use AH in Transport Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1021_01	**Test Purpose:**	TP_SEC_1021_01
Summary:	'IPsec Host support of ESP tunnel mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1021, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
       }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Tunnel Mode to secure all communications to and from QE1 b. QE1 will use ESP in Tunnel Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1021_02	**Test Purpose:**	TP_SEC_1021_02
Summary:	'IPsec Host support of AH tunnel mode'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_1021, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE1 using AH
                          with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                          with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Tunnel Mode to secure all communications to and from QE1 b. QE1 will use AH in Tunnel Mode to secure all communications to and from the EUT Security Association established from the EUT to QE1 Security Association established from QE1 to the EUT		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to the EUT		
2	Check: Does QE1 receive an Echo Reply from the EUT	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1022_01	**Test Purpose:**	TP_SEC_1022_01
Summary:	'IPsec Gateway support of ESP tunnel mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1022, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                          with the tunnel mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Tunnel Mode to secure all communications to and from QE4 b. QE4 will use ESP in Tunnel Mode to secure all communications to and from the EUT Security Association established from QE4 to EUT Security Association established from EUT to QE4

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_1022_02	**Test Purpose:**	TP_SEC_1022_02
Summary:	'IPsec Gateway support of AH tunnel mode'		
Roles:	Ipsec_gateway	**Configuration:**	CF_SEC_03
References:	RQ_002_1022, RQ_002_3040		

```
with {     EUT configured 'to protect all traffic to/from QE4 using AH
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                          with the tunnel mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH in Tunnel Mode to secure all communications to and from QE4 b. QE4 will use AH in Tunnel Mode to secure all communications to and from the EUT c. QE1 will only accept secure communication from QE2 d. QE2 will only accept secure communication from QE1 Security Association established from QE2 to QE1 Security Association established from QE1 to QE1

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to QE2		
2	Check: Does QE1 receive an Echo Reply from QE2?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_3000_01	**Test Purpose:**	TP_SEC_3000_01
Summary:	'IPsec host supports integrity-only ESP'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3000		

```
with {     EUT configured 'to protect communication with QE1 using only
                           the integrity service of ESP'
         and QE1 configured 'to accept only packets protected using only
                           the integrity service of ESP'
       }
  ensure that
    {
      when { EUT receives a packet  from QE1
                 indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:	Security Policy defined such that: a. EUT will protect communication with QE1 using only the integrity service of ESP b. QE1 will accept only packets protected by the integrity service of ESP A Security Association exists between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	Fail
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_3001_01	**Test Purpose:**	TP_SEC_3001_01
Summary:	'IPsec host supports full-service ESP'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3001		

```
with {     EUT configured 'to protect communication with QE1
                           using the confidentiality and integrity
                           services of ESP'
         and QE1 configured 'to accept only packets protected
                           using the confidentiality and integrity
                           services of ESP'
       }
  ensure that
    {
      when { EUT receives a packet  from QE1
                 indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:	Security Policy defined such that: a. EUT will protect communication with QE1 using the confidentiality and integrity services of ESP b. QE1 will accept only packets protected by the confidentiality and integrity services of ESP A Security Association exists between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	Fail
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_3002_01	**Test Purpose:**	TP_SEC_3002_01
Summary:	'IPsec host supports confidentiality-only ESP'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3002		

```
with {     EUT configured 'to protect communication with QE1
                          using only the confidentiality service of ESP'
        and QE1 configured 'to accept only packets protected
                          using only the confidentiality service of ESP'
      }
  ensure that
    {
      when { EUT receives a packet  from QE1
                 indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:	Security Policy defined such that: a. EUT will protect communication with QE1 using only the confidentiality service of ESP b. QE1 will accept only packets protected by the confidentiality service of ESP A Security Association exists between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_3013_01	**Test Purpose:**	TP_SEC_3013_01
Summary:	'IPsec host does not increment the sequence number to a value greater than the biggest 32-bit number'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3013		

```
with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and EUT configured 'to activate anti-replay'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and QE1 configured 'to activate anti-replay'
      and a Security_Association established between the EUT and QE1
    }
  ensure that
    {
      when { EUT is requested to send a packet containing a sequence_number
                  greater than 'the biggest 32-bit number' }
      then {     EUT deletes the established Security_Association to QE1
             and EUT establishes a new Security_Association to QE1 }
    }
```

Pre-test conditions:	NOT TESTABLE BY INTEROPERABILITY MEANS This would imply sending more than 4 000 000 000 packets…

Step	Test Sequence	Verdict	
		Pass	**Fail**
Observations:			

Test Description			
Identifier:	TD_SEC_3054_01	**Test Purpose:**	TP_SEC_3054_01
Summary:	'IPsec host maintains the sequence number ESP Security Associations across local reboots when anti-replay is activated'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3054		

```
with {     EUT configured 'to activate anti-replay'
         and EUT configured 'to protect its communication with QE1 using ESP'
         and QE1 configured 'to activate anti-replay'
         and QE1 configured 'to protect its communication with EUT using ESP'
         and an ESP Security_Association established
             between the EUT and QE1
       }
  ensure that
    {
      when { EUT is requested to reboot }
      then { QE1 is able to communicate with EUT after the reboot }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP to protect all of its communications with QE1 b. QE1 will use ESP to protect all of its communications with the EUT EUT is configured to activate anti-replay QE1 is configured to activate anti-replay A Security Association has been established between EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause the EUT to send 10 Echo Requests to QE1		
2	Reboot the EUT		
3	Cause QE1 to send an Echo Request to EUT		
4	Check: does QE1 receive an Echo Reply from EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_3061_01	**Test Purpose:**	TP_SEC_3061_01
Summary:	'IPsec host discards any packet containing an ESP Header that does not match any Security Association'		
Roles:	Ipsec_host, Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3061, RQ_002_3061, RQ_002_3091		

```
with {     EUT configured 'to use ESP to secure its communication with QE1'
         and EUT 'not having established any Security Association with QE1'
         and QE1 configured 'to use ESP to secure its communication with EUT'
       }
  ensure that
    {
      when { EUT receives a packet from QE1
               containing an ESP_Header
               indicating that a response is requested }
      then { EUT discards the packet
         and EUT sends no response to QE1 }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP to protect all of its communications with QE1 b. QE1 will use ESP to protect all of its communications with the EUT No Security Association is established between the EUT and QE1

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from EUT?	No	Yes
Observations:			

Test Description			
Identifier:	TD_SEC_3063_01	**Test Purpose:**	TP_SEC_3063_01
Summary:	'IPsec host supports anti-replay service'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3063, RQ_002_3068, RQ_002_3072		

```
with
    {     EUT configured 'to use integrity service of ESP
                          to secure its communication with QE1'
      and EUT configured 'to enable anti-replay'
      and QE1 configured 'to use integrity service of ESP
                          to secure its communication with EUT'
      and QE1 configured 'to enable anti-replay'
    }
  ensure that
    {
      when { EUT receives a packet from QE1
                  containing a previously used sequence_number
                  in the Authentication_Header }
      then { EUT sends no response to QE1 }
    }
```

Pre-test conditions:

Security Policy defined such that:

a. The EUT will secure all communications to QE1 and QE6 using the ESP integrity only service
b. QE1 will secure all communications to the EUT using the ESP integrity only service
c. QE6 will secure all communications to the EUT using the ESP integrity only service
d. The EUT will only accept communications from QE1 and QE6 if they are secured using the ESP integrity only service
e. QE1 will only accept communications from the EUT if they are secured using the ESP integrity only service
f. QE6 will only accept communications from the EUT if they are secured using the ESP integrity only service

EUT is configured to enable anti-replay
QE1 is configured to enable anti-replay
QE6 is configured to enable anti-replay
QE6 is configured with the same link-local address as QE1
QE1 is disconnected from Network
A security association has been established between the EUT and QE1
A security association has been established between the EUT and QE6 using identical parameters
to those set for the SA between the EUT and QE1

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE6 to send an Echo Request to EUT		
2	Check: does QE6 receive an Echo Reply from EUT?	Yes	No
3	Disconnect QE6 from Network B		
4	Connect QE1 to Network B		
5	Cause QE1 to send an Echo Request to EUT		
6	Check: does QE1 receive an Echo Reply from EUT?	No	Yes

Observations:

Test Description			
Identifier:	TD_SEC_3064_01	**Test Purpose:**	TP_SEC_3064_01
Summary:	'IPsec host does not enable anti-replay service when integrity service is not enabled for the Security_Association'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3064		

```
with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and EUT configured 'with the integrity service disabled'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and QE1 configured 'with the integrity service disabled'
      and a Security_Association established between the EUT and QE1
    }
  ensure that
    {
      when { EUT receives a packet from QE1
                  containing a previously used sequence_number
                             in the Authentication_Header
             and indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:

Security Policy defined such that:

a. The EUT will secure all communications to QE1 and QE6 using ESP but not the integrity only service
b. QE1 will secure all communications to the EUT using ESP but not the integrity only service
c. QE6 will secure all communications to the EUT using ESP but not the integrity only service
d. The EUT will only accept communications from QE1and QE6 if they are secured using ESP
e. QE1 will only accept communications from the EUT if they are secured using ESP
f. QE6 will only accept communications from the EUT if they are secured using ES

The EUT is configured to enable anti-replay
QE1 is configured to enable anti-replay
QE6 is configured to enable anti-replay
QE6 is configured with the same link-local address as QE1
QE1 is disconnected from Network
A security association has been established between the EUT and QE1
A security association has been established between the EUT and QE6 using identical parameters to those set for the SA between the EUT and QE1

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE6 to send an Echo Request to EUT		
2	Check: does QE6 receive an Echo Reply from EUT?	Yes	No
3	Disconnect QE6 from Network B		
4	Connect QE1 to Network B		
5	Cause QE1 to send an Echo Request to EUT		
6	Check: does QE1 receive an Echo Reply from EUT?	Yes	No

Observations:

Test Description			
Identifier:	TD_SEC_3065_01	**Test Purpose:**	TP_SEC_3065_01
Summary:	'IPsec host does not check Sequence Number on Multisender ESP Security Associations'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_3065		

```
with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and a Multisender_Security_Association established
          between the EUT and QE1
    }
  ensure that
    { when { EUT receives a packet from QE1
                containing a previously used sequence_number
                           in the Authentication_Header
           and indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will secure its communication with QE1 using ESP b. QE1 will secure its communication with EUT using ESP c. QE6 will secure its communication with EUT using ESP A Multisender Security Association has been established between the EUT (as the recipient) and both QE1 and QE6 (as the senders)

Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE6 to send an Echo Request to EUT		
2	Check: does QE6 receive an Echo Reply from EUT?	Yes	No
3	Cause QE1 to send an Echo Request to EUT		
4	Check: does QE1 receive an Echo Reply from EUT?	Yes	No
Observations:			

Group 4: RFC 4302 - IP Authentication Header (AH)

Test Description			
Identifier:	TD_SEC_2014_01	**Test Purpose:**	TP_SEC_2014_01
Summary:	'IPsec host does not increment the sequence number to a value greater than the biggest 32-bit number'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_2014		

```
with {     EUT configured 'to use Authentication Header to secure
                          its communication with QE1'
         and EUT configured 'to activate anti-replay'
         and QE1 configured 'to use Authentication Header to secure
                          its communication with EUT'
         and QE1 configured 'to activate anti-replay'
         and a Security_Association established between the EUT and QE1
       }
  ensure that
    {
      when { EUT is requested to send a packet containing a sequence_number
                greater than 'the biggest 32-bit number' }
      then {     EUT deletes the established Security_Association to QE1
             and EUT establishes a new Security_Association to QE1 }
    }
```

Pre-test conditions:	NOT TESTABLE BY INTEROPERABILITY MEANS This would imply sending more than 4 000 000 000 packets…		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
Observations:			

Test Description			
Identifier:	TD_SEC_2046_01	**Test Purpose:**	TP_SEC_2046_01
Summary:	'IPsec host discards any packet containing an Authentication Header that does not match any Security Association'		
Roles:	Ipsec_host, Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_2046, RQ_002_2046		

```
with {     EUT configured 'to use Authentication Header to secure
                          its communication with QE1'
         and EUT 'not having established any Security Association with QE1'
         and QE1 configured 'to use Authentication Header to secure
                          its communication with EUT'
       }
  ensure that
    {
      when { EUT receives a packet from QE1
               containing an Authentication_Header
               indicating that a response is requested }
      then { EUT discards the packet
         and EUT sends no response to QE1 }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH to secure all of its communications with QE1 b. QE1 will use AH to secure all of its communications with the EUT c. Security Associations between the EUT and QE1 will not be created automatically when needed The EUT has not established any Security Association with QE1		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from EUT?	No	Yes
Observations:			

Test Description			
Identifier:	TD_SEC_2057_01	**Test Purpose:**	TP_SEC_2057_01
Summary:	'IPsec host calculates Integrity Check Value and accepts the packet if it is the same as the ICV held in that packet'		
Roles:	Ipsec_host, Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_2057, RQ_002_2028, RQ_002_2057		

```
with
    {     EUT configured 'to use Authentication Header to secure
                          its communication with QE1'
      and QE1 configured 'to use Authentication Header to secure
                          its communication with EUT'
          and a Security_Association established between the EUT and QE1
    }
  ensure that
    { when { QE1 sends a packet to EUT
             containing an Authentication_Header
             indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }
```

Pre-test conditions:	Security Policy defined such that: a. The EUT will use AH to secure all of its communications with QE1 b. QE1 will use AH to secure all of its communications with the EUT The EUT has established a Security Association with QE1 QE1 has established a Security Association with the EUT

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Group 6: RFC 4305 Cryptographic Algorithm Implementation Requirements for ESP and AH

Test Description			
Identifier:	TD_SEC_5002_01	**Test Purpose:**	TP_SEC_5002_01
Summary:	'Support of NULL encryption algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5002		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with NULL encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with NULL encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with NULL encryption algorithm. b. QE1 will protect all traffic to/from the EUT using ESP with NULL encryption algorithm. A Security Association is established between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5003_01	**Test Purpose:**	TP_SEC_5003_01
Summary:	'Supports of TripleDES-CBC encryption algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5003		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with TripleDES-CBC encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with TripleDES-CBC encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with TripleDES-CBC encryption algorithm. b. QE1 will protect all traffic to/from the EUT using ESP with TripleDES-CBC encryption algorithm. A Security Association is established between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5004_01	**Test Purpose:**	TP_SEC_5004_01
Summary:	'Support of AES-CBC encryption algorithm with 128-bit key length'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5004		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with AES-CBC encryption algorithm and with 128-bit key length'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with AES-CBC encryption algorithm and with
                          128-bit key length'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with ES-CBC encryption algorithm with 128-bit key length b. QE1 will protect all traffic to/from the EUT using ESP with ES-CBC encryption algorithm with 128-bit key length A Security Association is established between the EUT and QE1 (both directions)

Step	Test Sequence	Verdict	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5005_01	**Test Purpose:**	TP_SEC_5005_01
Summary:	'Support of AES-CTR encryption algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5005		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with AES-CTR encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with AES-CTR encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with AES-CTR encryption algorithm b. QE1 will protect all traffic to/from the EUT using ESP with AES-CTR encryption algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5007_01	**Test Purpose:**	TP_SEC_5007_01
Summary:	'Support of HMAC-SHA1 authentication algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5007		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with HMAC-SHA1 authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with HMAC-SHA1 authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with HMAC-SHA1 authentication algorithm b. QE1 will protect all traffic to/from the EUT using ESP with HMAC-SHA1 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5008_01	**Test Purpose:**	TP_SEC_5008_01
Summary:	'Support of NULL authentication algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5008		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with NULL authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with NULL authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with NULL authentication algorithm b. QE1 will protect all traffic to/from the EUT using ESP with NULL authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5009_01	**Test Purpose:**	TP_SEC_5009_01
Summary:	'Support of AES-XCBC-MAC authentication algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5009		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                          with AES-XCBC-MAC authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                          with AES-XCBC-MAC authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with AES-XCBC-MAC-96 authentication algorithm b. QE1 will protect all traffic to/from the EUT using ESP with AES-XCBC-MAC-96 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5010_01	**Test Purpose:**	TP_SEC_5010_01
Summary:	'Support of HMAC-MD5 authentication algorithm'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5010		

```
with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                           with HMAC-MD5 authentication algorithm'
         and QE1 configured 'to protect all traffic to/from QE1 using ESP
                           with HMAC-MD5 authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using ESP with HMAC-MD5 authentication algorithm b. QE1 will protect all traffic to/from the EUT using ESP with HMAC-MD5 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5012_01	**Test Purpose:**	TP_SEC_5012_01
Summary:	'Support of HMAC-SHA1 as authentication algorithm for AH'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5012		

```
with {     EUT configured 'with HMAC-SHA1 as authentication algorithm for
                           Authentication Header '
         and QE1 configured 'with HMAC-SHA1 as authentication algorithm for
                           Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using AH with HMAC-SHA1 authentication algorithm b. QE1 will protect all traffic to/from the EUT using AH with HMAC-SHA1 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

Test Description			
Identifier:	TD_SEC_5013_01	**Test Purpose:**	TP_SEC_5013_01
Summary:	'Support of AES-XCBC-MAC as authentication algorithm for AH'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5013		

```
with {     EUT configured 'with AES-XCBC-MAC as authentication algorithm
                           for Authentication Header '
         and QE1 configured 'with AES-XCBC-MAC as authentication algorithm
                           for Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using AH with AES-XCBC-MAC-96 authentication algorithm b. QE1 will protect all traffic to/from the EUT using AH with AES-XCBC-MAC-96 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

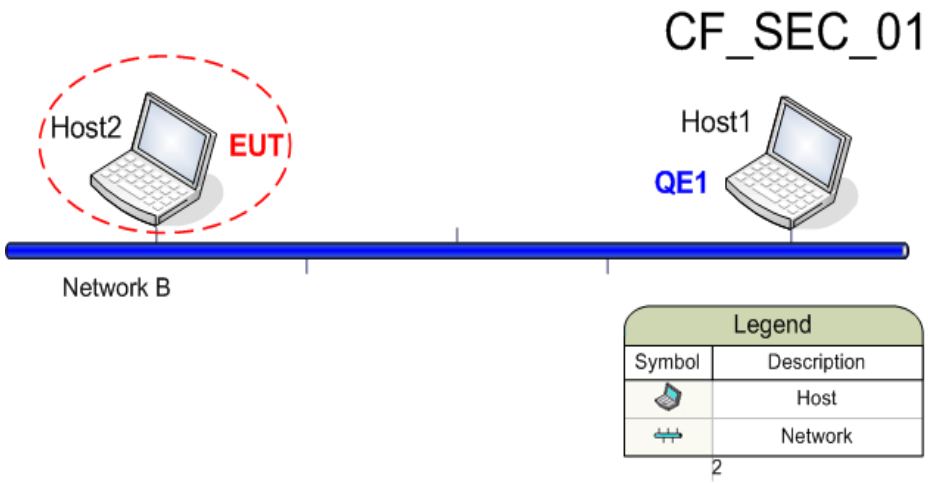
Test Description			
Identifier:	TD_SEC_5014_01	**Test Purpose:**	TP_SEC_5014_01
Summary:	'Support of HMAC-MAC as authentication algorithm for AH'		
Roles:	Ipsec_host	**Configuration:**	CF_SEC_01
References:	RQ_002_5014		

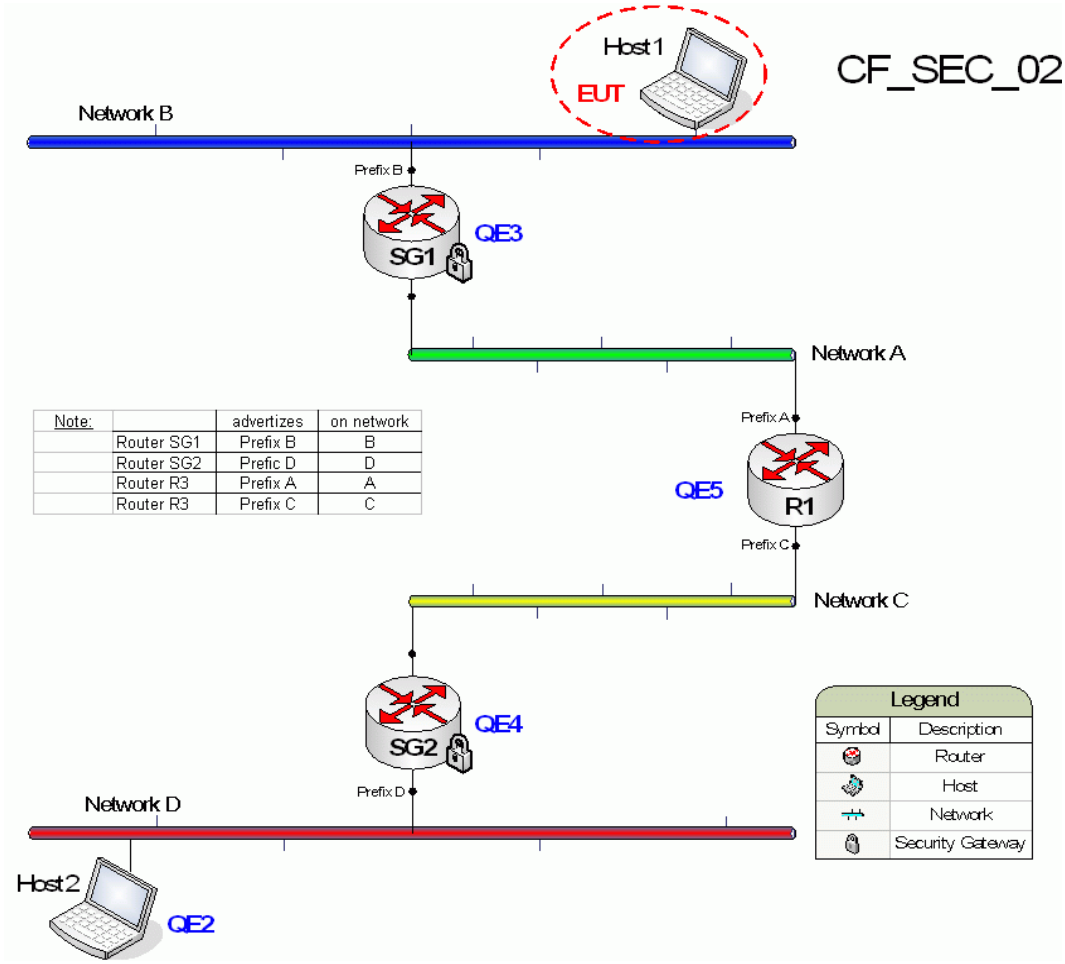
```
with {     EUT configured 'with HMAC-MAC as authentication algorithm for
                           Authentication Header '
         and QE1 configured 'with HMAC-MAC as authentication algorithm for
                           Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }
```

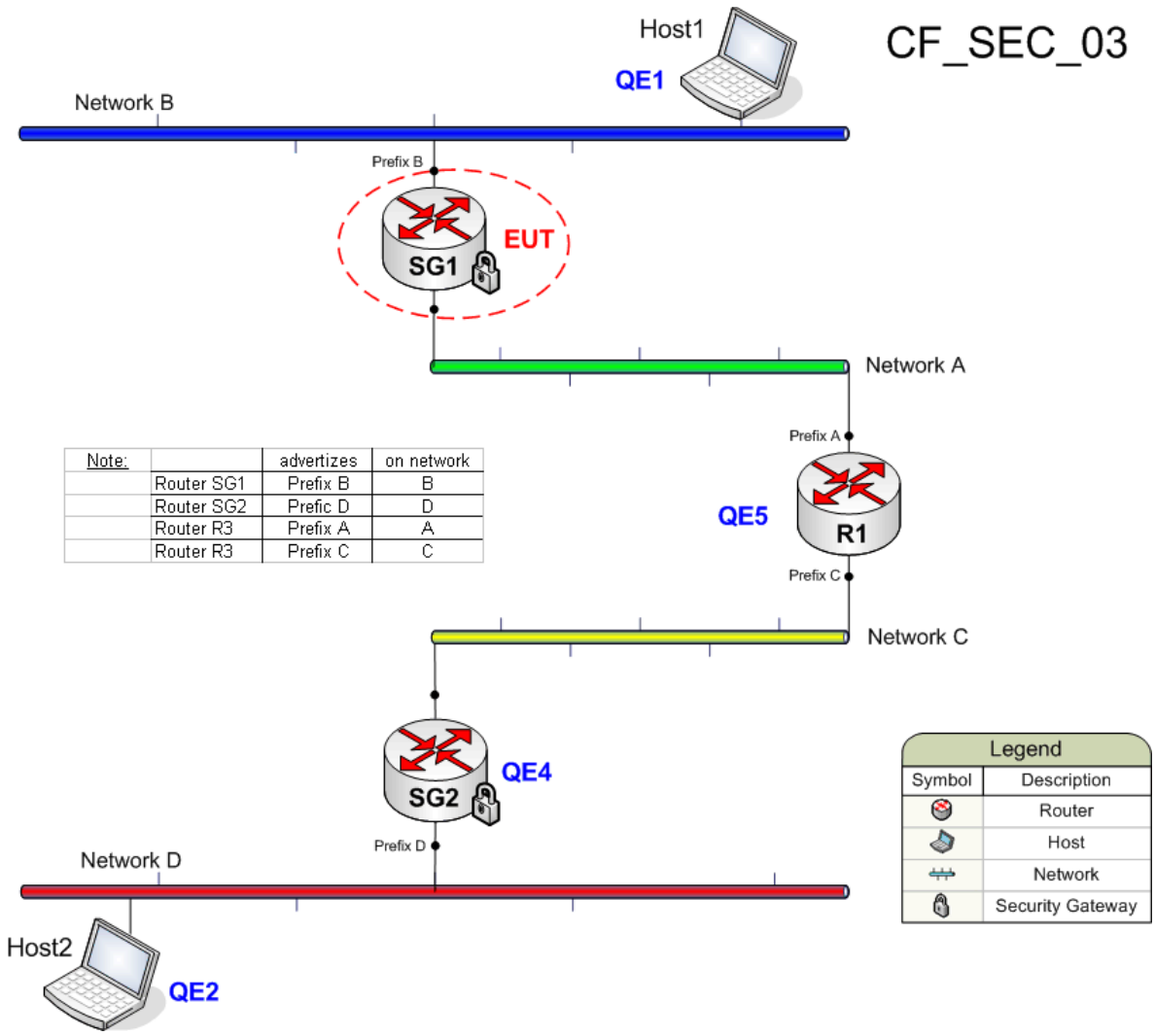
Pre-test conditions:	Security Policy is defined such that: a. The EUT will protect all traffic to/from QE1 using AH with HMAC-MAC-96 authentication algorithm b. QE1 will protect all traffic to/from the EUT using AH with HMAC-MAC-96 authentication algorithm A Security Association is established between the EUT and QE1 (both directions)		
Step	**Test Sequence**	**Verdict**	
		Pass	**Fail**
1	Cause QE1 to send an Echo Request to EUT		
2	Check: does QE1 receive an Echo Reply from the EUT?	Yes	No
Observations:			

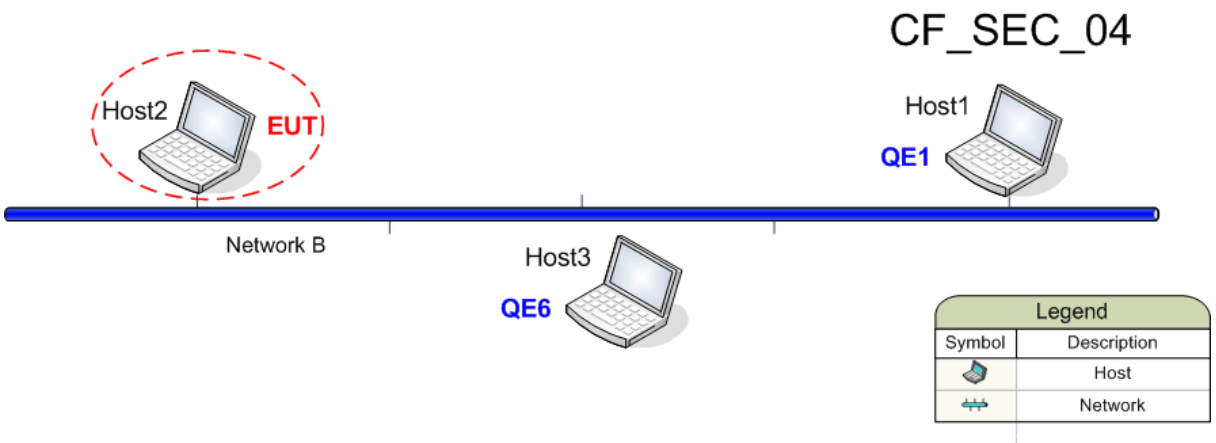
Annex A (informative): Interoperability Testing Configurations

The following architectural configurations are referenced in the IPv6 Security Interoperability Test Descriptions specified in the present document. They are intended to give a general rather than specific view of the possible roles of the EUT and its associated QE(s) and the relationships between them.






CF_SEC_03
Host1
QE1
Network B
Prefix B
EUT
SG1
Network A
Prefix A
QE5
R1
Prefix C
Network C
QE4
SG2
Prefix D
Network D
Host2
QE2
Note:
Router SG1 advertizes Prefix B on network B
Router SG2 advertizes Prefic D on network D
Router R3 advertizes Prefix A on network A
Router R3 advertizes Prefix C on network C
Legend
Symbol Description
Router
Host
Network
Security Gateway


CF_SEC_04
Host2
EUT
Host1
QE1
Network B
Host3
QE6
Legend
Symbol Description
Host
Network

Annex B (informative): IPv6 Interoperability Test Purposes

The Test Suite Structure is based on the IPv6 Security RFCs and the IPv6 Requirements Catalogue nodes. It is defined by the groups within the following TPLan specification of test purposes. The numbering is not contiguous so that new TPs can be added at a later date without the need to completely renumber the TSS groups.

```
TSS     : SEC
Title   : 'IPv6 Security Test Purposes'
Version : 1.0.0
Date    : 09.10.2006
Author  : 'STF276 - Task 4'

-- Last $Rev: 430 $
-- Last $Author: vreck $
-- $Date: 2007-03-15 16:25:18 +0100 (Thu, 15 Mar 2007) $

--***Cross references***

-- Requirements
xref RQ_002 {RFC4301,
             RFC4302,
             RFC4303,
             RFC4305,
             RFC4306}
xref RQ_001 {RFC3776}

-- Configurations
xref CF_SEC_01 {Configs_IOP_SEC.pdf}
xref CF_SEC_02 {Configs_IOP_SEC.pdf}
xref CF_SEC_03 {Configs_IOP_SEC.pdf}
xref CF_SEC_04 {Configs_IOP_SEC.pdf}

--***Definitions***

-- Entities
def entity EUT
def entity QE1
def entity QE2
def entity QE3
def entity QE4
def entity QE5
def entity QE6
def entity Security_Association
def entity Multisender_Security_Association

-- Messages
def event IKE_SA_INIT_request {proposal}
def event IKE_SA_INIT_response {proposal}
def event INFORMATION_Request
def event INFORMATION_Response
def event Notify_Payload {NO_PROPOSAL_CHOSEN}
def event DELETE_Payload {IKE_SA}
def event packet {Authentication_Header,
                  ESP_Header,
                  sequence_number}

def event reboot
def event response
def context {sends [no] ~response}

-- Values
def value ESP
def value lifetime
def value minute

-- Keywords - Preconditions
def word configured

-- Keywords - Actions
def word attempts
def word communicate
def word detects
```

```
def word establish
def word expiry
def word requested
def context {is ~requested to}
def word send
def word support

-- Keywords - Responses
def word deletes
def word discards
def word established
def word establishes
def word implemented
def word indicates
def word receipt
def context {~indicates ~receipt}
def word receive
def word rejects
def context {sends [no] ~response}
def context {receipt of [the] ~response}
def word using

-- Keywords - Glue
def word able
def word are
def word at
def word between
def word directly
def word even
def word for
def word greater
def word immediate
def word least
def word manually
def word more
def word new
def word offered
def word previously
def word securely
def context {~communicate ~securely}
def word than
def word unable
def word used


--*************************************************--
--* RFC4301  -  Security Architecture for the Internet Protocol
--*************************************************--

Group 1 'RFC4301 - Internet Security Architecture'

End Group 1

--*************************************************--
--* RFC4306  -  Internet Key Exchange (IKEv2) Protocol
--*************************************************--

Group 2 'RFC4306 - Internet Key Exchange protocol (IKEv2)'

Group 2.1 'Informational Exchanges'

TP id   : TP_SEC_6010_01
summary : 'An IKE implementation should close a Security Associations upon
           receipt of an INFORMATION request with a Delete payload identifying
           that particular SA'
RQ ref  : RQ_002_6010
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6010_01
with {     EUT configured 'to accept traffic from QE1 only if secured'
       and QE1 'having successfully established multiple Child_SAs with EUT'
     }
ensure that {
  when  { EUT receives an INFORMATION_Request from QE1
          containing a DELETE_payload
          for a security_association between QE1 and the EUT}
  then  { QE1 and EUT are unable to communicate securely
                  using that security_association}
```

```
            }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6011_01
summary : 'An IKE implementation should delete Child_SAs when the
           associated IKE_SA is deleted'
RQ ref  : RQ_002_6011
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6011_01
with {      EUT configured 'to accept traffic only if secured'
        and QE1 'having successfully established a single IKE SA with EUT'
        and QE1 'having successfully established some CHILD SAs with EUT'
     }
ensure that {
  when  { EUT receives an INFORMATION_Request from the EUT
          containing a DELETE_payload
          for the IKE_SA between QE1 and the EUT}
  then  { QE1 and EUT are unable to communicate securely }
          }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6041_01
summary : 'An IKE endpoint should accept and process requests while it is
           waiting for responses to its own requests'
RQ ref  : RQ_002_6041
Role    : IPsec_host
config  : CF_SEC_04
TD ref  : TD_SEC_6041_01
with {      EUT configured 'only to communicate securely with QE1'
        and EUT configured 'only to communicate securely with QE6'
     }
ensure that {
  when {    EUT sends an IKE_SA_INIT_Request to QE6
       and QE6 is unable to send an immediate IKE_SA_INIT_Response to the EUT }
  then  { EUT and QE1 are able to communicate securely
          before the EUT receives an IKE_SA_INIT_Response from QE6 }
          }

End Group 2.1

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

Group 2.2 'Message Length'

TP id   : TP_SEC_6024_01
summary : 'An IKE implementation should be able to send IKE messages that are
           up to 1280 bytes long'
RQ ref  : RQ_002_6024
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6024_01
with {      EUT configured 'to use certificate authentication with
                            certificates leading to 1280 bytes long messages'
        and QE1 configured 'to support certificate authentication'
     }
ensure that {
  when  { EUT  sends an IKE_SA_INIT_Request to QE1 }
  then  { EUT and QE1 are able to communicate securely }
          }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6025_01
summary : 'An IKE implementation should be able to receive and process
           IKE messages that are up to 1280 bytes long'
RQ ref  : RQ_002_6025
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6025_01
with {      EUT configured 'to support certificate authentication'
        and QE1 configured 'to use certificate authentication with
                            certificates leading to 1280 bytes long messages'
     }
ensure that {
  when  { QE1 sends an IKE_SA_INIT_Request to the EUT }
```

```
  then  { EUT and QE1 are able to communicate securely }
            }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6026_01
summary : 'An IKE implementation should be able to send IKE messages that are
           up to 3000 bytes long'
RQ ref  : RQ_002_6026
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6026_01

with {      EUT configured 'to use certificate authentication with
                            certificates leading to 3000 bytes long messages'
        and QE1 configured 'to support certificate authentication'
     }
ensure that {
  when  { EUT sends an IKE_SA_INIT_Request to QE1 }
  then  { EUT and QE1 are able to communicate securely }
            }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6027_01
summary : 'An IKE implementation should be able to receive and process
           IKE messages that are up to 3000 bytes long'
RQ ref  : RQ_002_6027
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_6027_01

with {      EUT configured 'to support certificate authentication'
        and QE1 configured 'to use certificate authentication with
                            certificates leading to 3000 bytes long messages'
     }
ensure that {
  when  { QE1 sends an IKE_SA_INIT_Request to the EUT }
  then  { EUT and QE1 are able to communicate securely }
            }

End Group 2.2

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxx--

Group 2.3 'Security Parameter Negotiation'
Group 2.3.1 'Algorithm negotiation'

TP id   : TP_SEC_6372_01
Summary : 'An IKE implementation selects a single security proposal from the
           set of proposals received from the other endpoint in a
           Security Association'
RQ ref  : RQ_002_6372
Role    : Host
config  : CF_SEC_01
TD ref  : TD_SEC_6372_01

with { EUT configured 'to support at least one of the security proposals
                       available to QE1'
     }
ensure that {
  when  { the EUT receives an IKE_SA_INIT_request from QE1
                containing at least 1 proposal
      and the EUT is able to support at least 1 proposal }
  then  { the EUT establishes a Security_Association to QE1
                        using 1 proposal }
            }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6372_02
Summary : 'An IKE implementation is unable to select a security proposal
           from the set of proposals received from the other endpoint in a
           Security Association'
RQ ref  : RQ_002_6372
Role    : Host
config  : CF_SEC_01
TD ref  : TD_SEC_6372_02
```

```
with { EUT configured 'so that it does not support any of the security
                       proposals available to QE1'
     }
ensure that {
  when  { the EUT receives an IKE_SA_INIT_request from QE1
                  containing at least 1 proposal
      and the EUT is unable to support even 1 proposal }
  then  { the EUT rejects the IKE_SA_INIT_request
                  indicating NO_PROPOSAL_CHOSEN }
             }

End Group 2.3.1

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

Group 2.3.2 'Security Association Lifetime'

TP id   : TP_SEC_6096_01
Summary : 'A Security Association is replaced if there is a continuing demand
           after the lifetime of the SA has expired'
RQ ref  : RQ_002_6096
Role    : Host
config  : CF_SEC_01
TD ref  : TD_SEC_6096_01

with  {  a Security_Association established between the EUT and QE1
       and 'regular secure traffic flowing between the EUT and QE1'
      }
ensure that {
  when  { the EUT detects the expiry of the lifetime of the Security_Association
          between the EUT and QE1 }
  then  { the EUT and QE1 are able to communicate securely }
          }

End Group 2.3.2


Group 2.3.4 'Generating keying material'

-- No IOP tests here

End Group 2.3.4
End Group 2.3

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

Group 2.4 'NAT Traversal'

TP id   : TP_SEC_6206_01
Summary : 'An IKE endpoint accepts messages with any UDP Source port'
RQ ref  : RQ_002_6206
Role    : Host
config  : CF_SEC_02
TD ref  : TD_SEC_6206_01

with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
    and QE3 configured 'to translate UDP Source Port numbers for NAT traversal'
    and QE4 configured 'to translate UDP Source Port numbers for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
          }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6212_01
Summary : 'An IKE endpoint sets UDP Destination Port number in IKE responses
           to the UDP Source Port number from the associated IKE request'
RQ ref  : RQ_002_6212
Role    : Host
config  : CF_SEC_02
TD ref  : TD_SEC_6212_01

with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
```

```
    and QE3 configured 'to translate UDP Source Port numbers for NAT traversal'
    and QE4 configured 'to translate UDP Source Port numbers for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
        }

--xxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_6213_01
Summary : 'An IKE endpoint sets IPv6 Destination Address in IKE responses
           to the IPv6 Source Address from the associated IKE request'
RQ ref  : RQ_002_6213
Role    : Host
config  : CF_SEC_02
TD ref  : TD_SEC_6213_01

with  { EUT configured 'only to communicate securely with QE2'
    and QE2 configured 'on to communicate securely with the EUT'
    and QE3 configured 'to translate IPv6 Source Addresses for NAT traversal'
    and QE4 configured 'to translate IPv6 Source Addresses for NAT traversal'
      }
ensure that {
  when  { a Security_Association is established between the EUT and QE2 }
  then  { EUT and QE2 are able to communicate securely }
        }

End Group 2.4

--xxxxxxxxxxxxxxxxxxxxxxxxxxx--

Group 2.5 'Retransmission Timers'

TP id   : TP_SEC_6031_01
Summary : 'An IKE endpoint is able to identify and process a received response
           to any of its IKE request'
RQ ref  : RQ_002_6031
Role    : Host
config  : CF_SEC_04
TD ref  : TD_SEC_6031_01

with  {    EUT configured 'only to communicate securely with QE1'
       and EUT configured 'only to communicate securely with QE6'
       and QE6 configured 'only to communicate securely with EUT'
       and QE1 configured 'only to communicate securely with the EUT'
       and 'continual communication established between the EUT and QE6'
      }
ensure that {
  when { EUT establishes a Security_Association to QE1 }
  then { EUT and QE2 are able to communicate securely }
        }

End Group 2.5
End Group 2


--************************************************--
--* RFC4303  -  IP Encapsulating Security Payload (ESP)
--************************************************--

Group 3 'RFC4303  -  IP Encapsulating Security Payload (ESP)'
-- TB & AMB

TP id   : TP_SEC_3063_01
summary : 'IPsec host supports anti-replay service'
RQ ref  : RQ_002_3063 , RQ_002_3068 , RQ_002_3072
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3063_01

  with
    {     EUT configured 'to use integrity service of ESP
                          to secure its communication with QE1'
      and EUT configured 'to enable anti-replay'
      and QE1 configured 'to use integrity service of ESP
                          to secure its communication with EUT'
      and QE1 configured 'to enable anti-replay'
```

```
    }
  ensure that
    {
      when { EUT receives a packet from QE1
                containing a previously used sequence_number
                in the Authentication_Header }
      then { EUT sends no response to QE1 }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3061_01
summary : 'IPsec host discards any packet containing an ESP Header
           that does not match any Security Association'
RQ ref  : RQ_002_3061
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3061_01

  with {     EUT configured 'to use ESP to secure its communication with QE1'
         and EUT 'not having established any Security Association with QE1'
         and QE1 configured 'to use ESP to secure its communication with EUT'
       }
  ensure that
    {
      when { EUT receives a packet from QE1
               containing an ESP_Header
               indicating that a response is requested }
      then { EUT discards the packet
         and EUT sends no response to QE1 }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3054_01
summary : 'IPsec host maintains the sequence number
           ESP Security Associations across local reboots when anti-replay
           is activated'
RQ ref  : RQ_002_3054
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3054_01

  with {     EUT configured 'to activate anti-replay'
         and EUT configured 'to protect its communication with QE1 using ESP'
         and QE1 configured 'to activate anti-replay'
         and QE1 configured 'to protect its communication with EUT using ESP'
         and an ESP Security_Association established
             between the EUT and QE1
       }
  ensure that
    {
      when { EUT is requested to reboot }
      then { QE1 is able to communicate with EUT after the reboot }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3002_01
summary : 'IPsec host supports confidentiality-only ESP'
RQ ref  : RQ_002_3002
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3002_01

  with {     EUT configured 'to protect communication with QE1
                             using only the confidentiality service of ESP'
         and QE1 configured 'to accept only packets protected
                             using only the confidentiality service of ESP'
       }
  ensure that
    {
```

```
      when { EUT receives a packet  from QE1
                  indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3001_01
summary : 'IPsec host supports full-service ESP'
RQ ref  : RQ_002_3001
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3001_01

  with {     EUT configured 'to protect communication with QE1
                             using the confidentiality and integrity
                             services of ESP'
         and QE1 configured 'to accept only packets protected
                             using the confidentiality and integrity
                             services of ESP'
       }
  ensure that
    {
      when { EUT receives a packet  from QE1
                  indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3000_01
summary : 'IPsec host supports integrity-only ESP'
RQ ref  : RQ_002_3000
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3000_01

  with {     EUT configured 'to protect communication with QE1 using only
                             the integrity service of ESP'
         and QE1 configured 'to accept only packets protected using only
                             the integrity service of ESP'
       }
  ensure that
    {
      when { EUT receives a packet  from QE1
                  indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }



--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3013_01
summary : 'IPsec host does not increment the sequence number to a value
           greater than the biggest 32-bit number'
RQ ref  : RQ_002_3013
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3013_01

  with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and EUT configured 'to activate anti-replay'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and QE1 configured 'to activate anti-replay'
      and a Security_Association established between the EUT and QE1
    }
  ensure that
    {
      when { EUT is requested to send a packet containing a sequence_number
                   greater than 'the biggest 32-bit number' }
      then {     EUT deletes the established Security_Association to QE1
```

```
            and EUT establishes a new Security_Association to QE1 }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3064_01
summary : 'IPsec host does not enable anti-replay service when
           integrity service is not enabled for the Security
           Association'
RQ ref  : RQ_002_3064
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3064_01

  with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and EUT configured 'with the integrity service disabled'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and QE1 configured 'with the integrity service disabled'
      and a Security_Association established between the EUT and QE1
    }
  ensure that
    {
      when { EUT receives a packet from QE1
                  containing a previously used sequence_number
                             in the Authentication_Header
             and indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_3065_01
summary : 'IPsec host does not check Sequence Number on Multisender ESP
           Security Associations'
RQ ref  : RQ_002_3065
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_3065_01

  with
    {     EUT configured 'to use ESP to secure its communication with QE1'
      and QE1 configured 'to use ESP to secure its communication with EUT'
      and a Multisender_Security_Association established
          between the EUT and QE1
    }
  ensure that
    { when { EUT receives a packet from QE1
                  containing a previously used sequence_number
                             in the Authentication_Header
             and indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }

End Group 3

--************************************************--
--* RFC4302  -  IP Authentication Header
--************************************************--

Group 4 'RFC4302 - IP Authentication Header'
-- TB & AMB


TP id   : TP_SEC_2046_01
summary : 'IPsec host discards any packet containing an Authentication Header
           that does not match any Security Association'
RQ ref  : RQ_002_2046
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_2046_01

  with {     EUT configured 'to use Authentication Header to secure
                             its communication with QE1'
```

```
        and EUT 'not having established any Security Association with QE1'
        and QE1 configured 'to use Authentication Header to secure
                            its communication with EUT'
      }
  ensure that
    {
      when { EUT receives a packet from QE1
               containing an Authentication_Header
               indicating that a response is requested }
      then { EUT discards the packet
         and EUT sends no response to QE1 }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_2014_01
summary : 'IPsec host does not increment the sequence number to a value
           greater than the biggest 32-bit number'
RQ ref  : RQ_002_2014
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_2014_01

  with {     EUT configured 'to use Authentication Header to secure
                             its communication with QE1'
        and EUT configured 'to activate anti-replay'
        and QE1 configured 'to use Authentication Header to secure
                            its communication with EUT'
        and QE1 configured 'to activate anti-replay'
        and a Security_Association established between the EUT and QE1
       }
  ensure that
    {
      when { EUT is requested to send a packet containing a sequence_number
                  greater than 'the biggest 32-bit number' }
      then {     EUT deletes the established Security_Association to QE1
             and EUT establishes a new Security_Association to QE1 }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_2057_01
summary : 'IPsec host calculates Integrity Check Value and accepts
           the packet if it is the same as the ICV held in that packet'
RQ ref  : RQ_002_2057
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_2057_01

  with
    {     EUT configured 'to use Authentication Header to secure
                          its communication with QE1'
      and QE1 configured 'to use Authentication Header to secure
                          its communication with EUT'
        and a Security_Association established between the EUT and QE1
    }
  ensure that
    { when { QE1 sends a packet to EUT
               containing an Authentication_Header
               indicating that a response is requested }
      then { QE1 indicates receipt of the response }
    }

End Group 4

--************************************************--
--* RFC4305  -  Cryptographic Algorithm Implementation Requirements for ESP and AH
--************************************************--

Group 6 'RFC4305  -  Cryptographic Algorithm Implementation Requirements
                     for ESP and AH'
-- LV & AB
```

```
TP id   : TP_SEC_1004_01
summary : 'Support of ESP'
RQ ref  : RQ_002_1004
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1004_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP'
         and QE1 configured 'to protect all traffic to/from EUT using ESP'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1005_01
summary : 'Support of AH'
RQ ref  : RQ_002_1005
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1005_01

  with {     EUT configured 'to protect all traffic to/from QE1 using AH'
         and QE1 configured 'to protect all traffic to/from EUT using AH'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1020_01
summary : 'IPsec Host support of ESP transport mode'
RQ ref  : RQ_002_1020, RQ_002_3039
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1020_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                            with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                            with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1020_02
summary : 'IPsec Host support of AH transport mode'
RQ ref  : RQ_002_1020, RQ_002_3039
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1020_02

  with {     EUT configured 'to protect all traffic to/from QE1 using AH
                            with the transport mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                            with the transport mode'
       }
  ensure that
    { when { a Security_Association is established between EUT and QE1 }
      then { QE1 is able to communicate with EUT }
    }
```

```
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1021_01
summary : 'IPsec Host support of ESP tunnel mode'
RQ ref  : RQ_002_1021, RQ_002_3040
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1021_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                             with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                             with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
       }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1021_02
summary : 'IPsec Host support of AH tunnel mode'
RQ ref  : RQ_002_1021, RQ_002_3040
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_1021_02

  with {     EUT configured 'to protect all traffic to/from QE1 using AH
                             with the tunnel mode'
         and QE1 configured 'to protect all traffic to/from EUT using AH
                             with the tunnel mode'
       }
  ensure that
       { when { a Security_Association is established between EUT and QE1 }
         then { QE1 is able to communicate with EUT }
      }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1022_01
summary : 'IPsec Gateway support of ESP tunnel mode'
RQ ref  : RQ_002_1022, RQ_002_3040
Role    : IPsec_Gateway
config  : CF_SEC_03
TD ref  : TD_SEC_1022_01

with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                          with the tunnel mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1022_02
summary : 'IPsec Gateway support of AH tunnel mode'
RQ ref  : RQ_002_1022, RQ_002_3040
Role    : IPsec_Gateway
config  : CF_SEC_03
TD ref  : TD_SEC_1022_02

with {     EUT configured 'to protect all traffic to/from QE4 using AH
                          with the tunnel mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                          with the tunnel mode'
```

```
     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1023_01
summary : 'IPsec Gateway Support of ESP transport mode'
RQ ref  : RQ_002_1023, RQ_002_3039
Role    : IPsec_Gateway
config  : CF_SEC_03
TD ref  : TD_SEC_1023_01

with {     EUT configured 'to protect all traffic to/from QE4 using ESP
                           with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using ESP
                           with the transport mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_1023_02
summary : 'IPsec Gateway Support of AH transport mode'
RQ ref  : RQ_002_1023, RQ_002_3039
Role    : IPsec_Gateway
config  : CF_SEC_03
TD ref  : TD_SEC_1023_02

with {     EUT configured 'to protect all traffic to/from QE4 using AH
                           with the transport mode'
       and QE4 configured 'to protect all traffic to/from EUT using AH
                           with the transport mode'

     }
ensure that
     { when { a Security_Association is established between EUT and QE4 }
       then { QE1 and QE2 are able to communicate }
     }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5002_01
summary : 'Support of NULL encryption algorithm'
RQ ref  : RQ_002_5002
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5002_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                            with NULL encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                            with NULL encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5003_01
```

```
summary : 'Supports of TripleDES-CBC encryption algorithm'
RQ ref  : RQ_002_5003
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5003_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                             with TripleDES-CBC encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                             with TripleDES-CBC encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5004_01
summary : 'Support of AES-CBC encryption algorithm with 128-bit key length'
RQ ref  : RQ_002_5004
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5004_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                             with AES-CBC encryption algorithm and with 128-bit key length'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                             with AES-CBC encryption algorithm and with
                             128-bit key length'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5005_01
summary : 'Support of AES-CTR encryption algorithm'
RQ ref  : RQ_002_5005
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5005_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                             with AES-CTR encryption algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                             with AES-CTR encryption algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5007_01
summary : 'Support of HMAC-SHA1 authentication algorithm'
RQ ref  : RQ_002_5007
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5007_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                             with HMAC-SHA1 authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                             with HMAC-SHA1 authentication algorithm'
       }
```

```
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5008_01
summary : 'Support of NULL authentication algorithm'
RQ ref  : RQ_002_5008
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5008_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                            with NULL authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                            with NULL authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5009_01
summary : 'Support of AES-XCBC-MAC authentication algorithm'
RQ ref  : RQ_002_5009
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5009_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                            with AES-XCBC-MAC authentication algorithm'
         and QE1 configured 'to protect all traffic to/from EUT using ESP
                            with AES-XCBC-MAC authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5010_01
summary : 'Support of HMAC-MD5 authentication algorithm'
RQ ref  : RQ_002_5010
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5010_01

  with {     EUT configured 'to protect all traffic to/from QE1 using ESP
                            with HMAC-MD5 authentication algorithm'
         and QE1 configured 'to protect all traffic to/from QE1 using ESP
                            with HMAC-MD5 authentication algorithm'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx-- LAURENT


--TP id   : TP_SEC_5011_01
--summary : 'Null Algo cannot be used simultaneously for authentication
```

```
--           AND encryption'
--RQ ref  : RQ_002_5011
--Role    : IPsec_Host
--config  : CF_SEC_01
--TD ref  : TD_SEC_5011_01

-- This is not a requirement that applies to a network admin, not on an
-- implementation
-- ==> REMOVE FROM IOP LIST


--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--


TP id   : TP_SEC_5012_01
summary : 'Support of HMAC-SHA1 as authentication algorithm for AH'
RQ ref  : RQ_002_5012
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5012_01

  with {     EUT configured 'with HMAC-SHA1 as authentication algorithm for
                             Authentication Header '
         and QE1 configured 'with HMAC-SHA1 as authentication algorithm for
                             Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_5013_01
summary : 'Support of AES-XCBC-MAC as authentication algorithm for AH'
RQ ref  : RQ_002_5013
Role    : IPsec_Host
config  : CF_SEC_01
TD ref  : TD_SEC_5013_01

  with {     EUT configured 'with AES-XCBC-MAC as authentication algorithm
                             for Authentication Header '
         and QE1 configured 'with AES-XCBC-MAC as authentication algorithm
                             for Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx--

TP id   : TP_SEC_5014_01
summary : 'Support of HMAC-MAC as authentication algorithm for AH'
RQ ref  : RQ_002_5014
Role    : IPsec_host
config  : CF_SEC_01
TD ref  : TD_SEC_5014_01

  with {     EUT configured 'with HMAC-MAC as authentication algorithm for
                             Authentication Header '
         and QE1 configured 'with HMAC-MAC as authentication algorithm for
                             Authentication Header '
         and QE1 configured 'to accept traffic from/to EUT only if secured'
       }
  ensure that
    {
      when { a Security_Association is established between EUT and QE1 }
      then { QE1 and the EUT are able to communicate }
    }


End Group 6
```

Annex C (informative): Bilbiography

ETSI ES 202 553: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); IPv6 Testing: Methodology and Framework".

History

Document history		
V1.1.1	May 2007	Publication