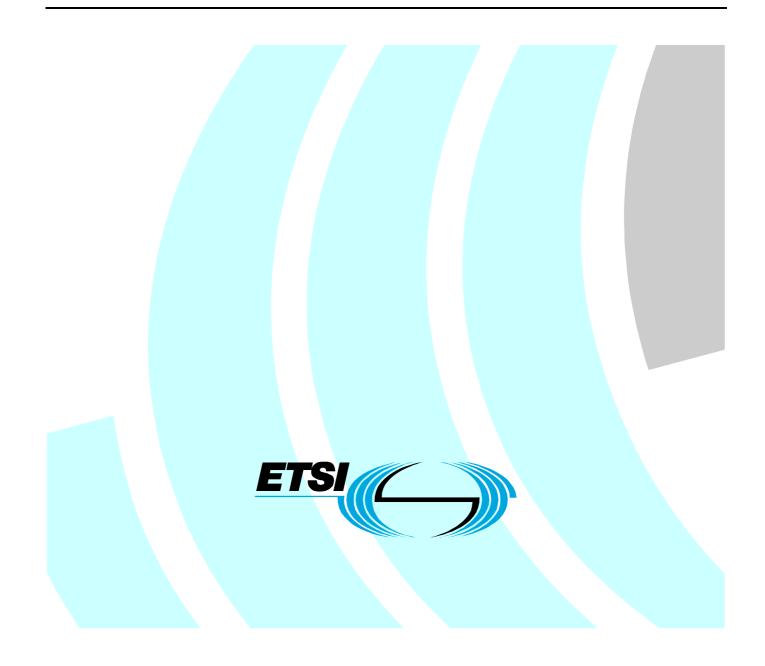
ETSI TS 102 597 V1.1.1 (2007-05)

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

Important notice

Individual copies of the present document can be downloaded from: http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services: <u>http://portal.etsi.org/chaircor/ETSI_support.asp</u>

Copyright Notification

No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

> © European Telecommunications Standards Institute 2007. All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members. **TIPHON**TM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members. **3GPP**TM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intelle	Intellectual Property Rights		
Forew	ord		4
Introd	uction		4
1	Scope		5
2	References		5
3	Abbreviations		5
4 4.1 4.1.1 4.2	Test Descriptions Index of test group	ability Test Specification	6 6
Anne	x A (informative):	Interoperability Testing Configurations	.38
Anne	x B (informative):	IPv6 Interoperability Test Purposes	.40
Anne	x C (informative):	Bilbiography	56
Histor	у		.57

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).

4

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
- TPLanTest 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.

Group 1: RFC 4301 - Internet Security Architecture	7
Group 2: RFC 4306 - Internet Key Exchange protocol (IKEv2)	
Group 2.1: Information Exchanges	
Group 2.2: Message Length	
Group 2.3: Security Parameter Negotiation	
Group 2.3.1: Algorithm Negotiation	
Group 2.3.2: Security Association Lifetime	
Group 2.3.3: Traffic Selector Negotiation	
Group 2.4: NAT Traversal	
Group 2.5: Retransmission Timers	20
Group 3: RFC 4303 - IP Encapsulating Security Protocol (ESP)	
Group 4: RFC 4302 - IP Authentication Header (AH)	
Group 6: RFC 4305 Cryptographic Algorithm Implementation Requirements for ESP and AH	

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_10	04_01			
Summary:	'Support of ESP'	·	•				
Roles:	Ipsec_host	Configuration:	CF_SEC_01				
References:	RQ_002_1004						
<pre>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 } } Protect all the form the term of the protect all traffic to/from QE1 using ESP' and QE1 and QE1 } communicate with EUT } } protect all traffic to to the protect all traffic to to the protect all traffic to the protect all traffi</pre>							
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 S	equence		Ver	dict		
		_		Pass	Fail		
1 Cause QE1 to send an Echo Request to EUT							
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No		
Observations:	•						

	Test Description					
Identifier:	TD_SEC_1005_01	Test Purpose:	TP_SEC_10	05_01		
Summary:	'Support of AH'	·				
Roles:	Ipsec_host	Configuration:	CF_SEC_01	l		
References:	RQ_002_1005					
<pre>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>						
Pre-test conditions:	 st 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 Se	quence		Ver	lict	
· ·		-		Pass	Fail	
1	Cause QE1 to send an Echo Request	to EUT				
2	Check: does QE1 receive an Echo Re	ply from the EUT?		Yes	No	
Observations:						

	Test Description				
Identifier:	TD_SEC_1020_01	Test Purpose:	TP_SEC_10	20_01	
Summary:	'IPsec Host support of ESP transport	mode'			
Roles:	Ipsec_host	Configuration:	CF_SEC_01	-	
References:	RQ_002_1020, RQ_002_3039				
<pre>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>					
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		equence		Verd	lict
-		•		Pass	Fail
1	Cause QE1 to establish a Security ass	sociation with EUT			
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No
Observations:		- ·		-	•

	Test Descr	iption			
Identifier:	TD_SEC_1020_02	Test Purpose:	TP_SEC_10	20_02	
Summary:	Psec Host support of AH transport mode'				
Roles:	Ipsec_host	Configuration:	CF_SEC_01	-	
References:	RQ_002_1020, RQ_002_3039				
and QE1 conf } ensure that { when { a Securi	<pre>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>				
	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	· ·	equence		Ver	dict
•		-		Pass	Fail
1	Cause QE1 to send an Echo Request	to the EUT			
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No
Observations:					-

	Test Description						
Identifier:	TD_SEC_1021_01	Test Purpose:	TP_SEC_10	21_01			
Summary:	'IPsec Host support of ESP tunnel mo						
Roles:	Ipsec_host	Configuration:	CF_SEC_01				
References:	RQ_002_1021, RQ_002_3040						
<pre>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>							
Pre-test conditions:	Pre-test conditions: Security Policy defined such that: a. The EUT will use ESP in Tunnel Mode to secure all communications to and from QE 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		quence		Verd	lict		
•		-		Pass	Fail		
1	Cause QE1 to send an Echo Request	to the EUT					
2	Check: Does QE1 receive an Echo Ro	eply from the EUT?		Yes	No		
Observations:							

	Test Descr	iption			
Identifier:	TD_SEC_1021_02	Test Purpose:	TP_SEC_10	21_02	
Summary:	'IPsec Host support of AH tunnel mo	de'	•		
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'					
<pre>ensure that { when { a Security_Association is established between EUT and QE1 } then { QE1 is able to communicate with EUT } }</pre>					
Pre-test conditions:	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 Se	equence		Ver	dict
•		•	ľ	Pass	Fail
1	Cause QE1 to send an Echo Request	to the EUT			
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No
Observations:					

	Test Description						
Identifier:	TD_SEC_1022_01	Test Purpose:	TP_SEC_10	22_01			
Summary:	'IPsec Gateway support of ESP tunne	el mode'					
Roles:	Ipsec_gateway	Configuration:	CF_SEC_03	3			
References:	RQ_002_1022, RQ_002_3040						
<pre>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>							
Pre-test conditions:	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	· · · · · ·	equence		Verd	lict		
•		•		Pass	Fail		
1	Cause QE1 to send an Echo Request	to QE2					
2	Check: Does QE1 receive an Echo R	eply from QE2?		Yes	No		
Observations:							

	Test Description					
Identifier:	TD_SEC_1022_02	Test Purpose:	TP_SEC_10)22_02		
Summary:	'IPsec Gateway support of AH tunnel	mode'				
Roles:	Ipsec_gateway	Configuration:	CF_SEC_03	3		
References:	RQ_002_1022, RQ_002_3040					
<pre>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'</pre>						
	rity_Association is established A QE2 are able to communicate }	between EUT and QE4	}			
Pre-test conditions:	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 QE1 to QE1 Security Association established from QE1 to QE1					
Step	Test Se	quence		Vere	lict	
		-		Pass	Fail	
1	Cause QE1 to send an Echo Request	to QE2				
2	Check: Does QE1 receive an Echo R	eply from QE2?		Yes	No	
Observations:						

	Test Descr	ription			
Identifier:	TD_SEC_1023_01	Test Purpose:	TP_SEC_10	23_01	
Summary:	'IPsec Gateway Support of ESP trans		•		
Roles:	Ipsec_gateway	Configuration:	CF_SEC_03	}	
References:	RQ_002_1023, RQ_002_3039				
<pre>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>					
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 Security Association established from QE4 to EUT Security Association established from EUT to QE4					
Step Test Sequence			Verdict		
~F		- 1 · · · · · ·		Pass	Fail
1	Cause QE1 to send an Echo Request	to QE2			
2	Check: Does QE1 receive an Echo R			Yes	No
Observations:					•

	Test Description							
Identifier:	TD_SEC_1023_02	Test Purpose:	TP_SEC_10	023_02				
Summary:	'IPsec Gateway Support of AH transp	Psec Gateway Support of AH transport mode'						
Roles:	Ipsec_gateway	Configuration:	CF_SEC_03	3				
References:	RQ_002_1023, RQ_002_3039							
and QE4 config } ensure that { when { a Secur then { QE1 and }	<pre>gured 'to protect all traffic to with the transport mode' gured 'to protect all traffic to with the transport mode' rity_Association is established d QE2 are able to communicate }</pre>	/from EUT using AH						
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 Se	equence		Vero	lict			
_				Pass	Fail			
1	Cause QE1 to send an Echo Request	to QE2						
2	Check: Does QE1 receive an Echo R	eply 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 Pur	pose: TP_SE	C_6010_01			
Summary:	'An IKE implementation should close a Securit	An IKE implementation should close a Security Associations upon receipt of an				
-	INFORMATION request with a Delete payload	l identifying that particu	ılar SA'			
Roles:	Ipsec_host Configu	ration: CF_SE	C_01			
References:	RQ_002_6010					
	gured 'to accept traffic from QE1 only if					
and QE1 'havi ۱	ng successfully established multiple Chil	d_SAs with EUT'				
ensure that {						
	es an INFORMATION_Request from QE1					
	ning a DELETE_payload)				
	security_association between QE1 and the I are unable to communicate securely	F.O.I. }				
	using that security_association}					
}	5 1 ,					
Pre-test conditions:	Security Policy defined such that:					
	a. QE1 will accept only secure communicat	ions from the EUT				
	b. The EUT will accept both secure and non-	-secure communication	s from QE1			
	c. QE1 will use ESP in Tunnel Mode for all	ICMP6 transmissions to	o the EUT			
	d. QE1 will use ESP in Transport Mode for	all UDP transmissions t	o the EUT			
Step	Test Sequence		Ver	dict		
			Pass	Fail		
1	Preamble: Cause the EUT to send an Echo Req	uest to QE1 (establishin	g			
	an IKE_SA with an ESP Tunnel Mode Child_S	A)				
2	Preamble: Check: Does the EUT receive an Ech	no Reply from QE1?	Yes	No		
3	Preamble: Cause the EUT to send Tracepath to	QE1 (establishing an				
	additional Child_SA using ESP in Tunnel Mod	e)				
4	Preamble: Check: Does the EUT receive a Trac	epath response indication	ng Yes	No		
	that QE1 was reached?		-			
5	Cause QE1 to delete the ESP Tunnel Mode CH	IILD_SA to the EUT				
6	Cause the EUT to send an Echo Request to QE	1				
7	Check: Does the EUT receive an Echo Reply fr	om QE1?	No	Yes		
8	Cause the EUT to send Tracepath to QE1					
9	Check: Does the EUT receive a Tracepath respo	onse indicating that QE	1 Yes	No		
				1		
,	was reached?					

	Test Descr	ption				
Identifier:	TD_SEC_6011_01	Test Purpose:	TP_SEC_601	1 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					
and QE1 'havi and QE1 'havi }	igured 'to accept traffic only if ing successfully established a s ing successfully established some	ngle IKE SA with EUT	,			
contair for the	es an INFORMATION_Request from th ning a DELETE_payload e IKE_SA between QE1 and the EUT F are unable to communicate secu					
Pre-test conditions:	Security Policy defined such that:					
	a. QE1 will accept only secure co					
	b. The EUT will accept both secur	e and non-secure commu	nications from	QE1		
Step	Test Se	quence		Ver	dict	
				Pass	Fail	
1	Cause the EUT to send an Echo Requ	est to QE1				
2	Check: Does the EUT receive an Ech	o Reply from QE1?		Yes	no	
3	Cause QE1 to delete the IKE_SA to t	ne EUT				
4	Cause the EUT to send an Echo Requ	est to QE1				
5	Check: Does the EUT receive an Ech	o Reply from QE1?		No	Yes	
Observations:	Untestable by IOP means					

	Те	st Description			
ldentifier:	TD_SEC_6041_01	Test Purpose:	TP_SEC_60	041_01	
Summary:	"An IKE endpoint should acc	cept and process requests whil	e it is waiting for	responses	s to its
-	own requests"		-	-	
Roles:	Host, Ipsec_host	Configuration:	CF_SEC_04	4	
References:	RQ_002_6041, RQ_002_604	41			
<pre> } ensure that { when { EUT send and QE6 is then then { EUT and QI before the } }</pre>	Eigured 'only to communicat ds an IKE_SA_INIT_Request f unable to send an immediate El are able to communicate e EUT receives an IKE_SA_IN	to QE6 e IKE_SA_INIT_Response to securely NIT_Response from QE6 }	the EUT }		
Pre-test conditions:		ity means. he IKE_SA_INIT_Response co huse NS will not work - so IKI			iot be
Step		Test Sequence		Ver	dict
_				Pass	Fail
Observations:	Untestable by IOP means				

Group 2.2: Message Length

Test Description							
Identifier:	TD_SEC_6024_01	Test Purpose:	TP_SEC_60	024_01			
Summary:	'An IKE implementation should be at	TIKE implementation should be able to send IKE messages that are up to 1 280 bytes long					
Roles:	Ipsec_host	Configuration:	CF_SEC_0	1			
References:	RQ_002_6024						
, i	with { EUT configured 'to use certificate authentication with certificates leading to 1 280 bytes long messages' and QE1 configured 'to support certificate authentication'						
	an IKE_SA_INIT_Request to QE1 } . are able to communicate secure]	Ly }					
Pre-test conditions:	 Security policy defined such that: a. The EUT will accept only secure b. QE1 will accept only secure cor c. The EUT will use certificate aut messages d. QE1 will support certificate aut 	nmunicaation from the E thentication with certifica	UT	o 1 280 byt	es long		
Step	Test Se	quence		Verd	lict		
				Pass	Fail		
1	Cause EUT to send an Echo Request Association establishment	to QE1, which leads to S	ecurity				
2	Check: Does EUT receive an Echo Ro	eply?		Yes	No		
Observations:		•		•	•		

	Test Descr	ription			
Identifier:	TD_SEC_6025_01	Test Purpose:	TP_SEC_60	025_01	
Summary:	'An IKE implementation should be at	ble to receive and process	SIKE message	es that are u	ıp to
-	1 280 bytes long'	-	-		-
Roles:	Ipsec_host	Configuration:	CF_SEC_01	-	
References:	RQ_002_6025				
and QE1 confi } ensure that { when { QE1 sends a	gured 'to support certificate au gured 'to use certificate authen certificates leading to : an IKE_SA_INIT_Request to the EU are able to communicate secure: Security policy defined such that: a. the EUT will accept only secure b. QE1 will accept only secure con c. QE1 will use certificate authent	ntication with 1 280 bytes long mess r } ly } e communication from Q mmunicaation from the E	E1 EUT	30 bytes lor	ng
	messages d. the EUT will support certificate	authentication			
Step	Test Se			Vere	dict
~~·· F		1		Pass	Fail
1	Cause QE1 to send an Echo Request Association establishment	to EUT, which leads to S	ecurity		
2	Check: Does QE1 receive an Echo Re	eply?		Yes	No
Observations:				•	•

	Test Descr	ription			
Identifier:	TD_SEC_6026_01	Test Purpose:	TP_SEC_6	026_01	
Summary:	'An IKE implementation should be al				es long'
Roles:	Ipsec_host	Configuration:	CF_SEC_0)1	
References:	RQ_002_6026		•		
and QEl confi } ensure that { when { EUT sends a	igured 'to use certificate auther certificates leading to igured 'to support certificate a an IKE_SA_INIT_Request to QE1 } I are able to communicate secure	3 000 bytes long me uthentication'	ssages '		
Pre-test conditions:	 Security policy defined such that: a. The EUT will accept only secure b. QE1 will accept only secure condition c. The EUT will use certificate au messages d. QE1 will support certificate aut 	mmunicaation from the thentication with certif	EUT	to 3 000 byt	es long
Step	Test Sequence			Ver	dict
~~~r		. <b>T</b>		Pass	Fail
1	Cause EUT to send an Echo Request Association establishment	to QE1, which leads to	Security		
2	Check: Does EUT receive an Echo R	eply?		Yes	No
Observations:		* *			

	Test Descr	iption				
Identifier:	TD_SEC_6027_01	Test Purpose:	TP_SEC_60	027_01		
Summary:	'An IKE implementation should be al	ble to receive and process	IKE message	es that are	up to	
	3 000 bytes long'	-	-		-	
Roles:	Ipsec_host	Configuration:	CF_SEC_0	1		
References:	RQ_002_6027		•			
and QE1 confi } ensure that { when { QE1 sends a	<pre>gured 'to support certificate a gured 'to use certificate auther certificates leading to an IKE_SA_INIT_Request to the EU are able to communicate secure Security policy defined such that: a. The EUT will accept only secure b. QE1 will accept only secure conduction and a secure only secure conduction b. QE1 will accept only secure conduction and a secure conduction a secure c</pre>	ntication with 3 000 bytes long messa T } ly } re communication from Q	 E1			
	<ul> <li>c. QE1 will use certificate authentication with certificates leading to 3 000 bytes long messages</li> <li>d. The EUT will support certificate authentication</li> </ul>					
Step	Test Se	equence		Ver	dict	
_				Pass	Fail	
1	Cause QE1 to send an Echo Request Association establishment	to EUT, which leads to Se	ecurity			
2	Check: Does QE1 receive an Echo Ro	eply?		Yes	No	
Observations:				•	•	

### Group 2.3: Security Parameter Negotiation

Group	2.3.1:	Algorithm	Negotiation
Oloup /	2.0.1.	/ ugonum	regoliulion

	Tes	t Description			
Identifier:	TD_SEC_6372_01	Test Purpose:	TP_SEC_6372_01		
Summary:	'An IKE implementation sele	cts a single security proposal	from the set of proposa	ls received	
	from the other endpoint in a S	Security Association'			
Roles:	Host, Host	<b>Configuration:</b>	CF_SEC_01		
References:	RQ_002_6372, RQ_002_637	2			
<pre>} ensure that {  when { the EUT re</pre>	d 'to support at least one available to QE1' cceives an IKE_SA_INIT_requ intaining at least 1 propos able to support at least tablishes a Security_Assoc using 1 proposal }	est from QE1 al 1 proposal }			
Pre-test conditions:	Untestable by IOP means				
Step		Test Sequence		Verdict	
			Pas	ss Fail	
Observations:					

	Т	est Description					
Identifier:	TD_SEC_6372_02	Test Purpose:	TP_SEC_63	372_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_63	372					
<pre>} ensure that {  when { the EUT r  c  and the EUT i  then { the EUT r  i </pre>	proposals available to eceives an IKE_SA_INIT_rea ontaining at least 1 propose s unable to support even 3 ejects the IKE_SA_INIT_rea ndicating NO_PROPOSAL_CHOS	quest from QE1 osal L proposal } quest SEN }					
Pre-test conditions:	b. QE1 will accept only	n that: only secure communications fro secure communications from th port any of the security proposa	ie EUT	E1			
Step		Test Sequence		Ver	dict		
		_		Pass	Fail		
1	Cause QE1 to send an Echo	request to EUT					
2	Check: Does QE1 receive a	n Echo Reply?		No	Yes		
<b>Observations:</b>							

	Test Descr	ription			
Identifier:	TD_SEC_6096_01	Test Purpose:	TP_SEC_6	096_01	
Summary:	'A Security Association is replaced if	there is a continuing de	emand after the	lifetime o	f the SA
	has expired'				
Roles:	Host	<b>Configuration:</b>	CF_SEC_0	1	
References:	RQ_002_6096				
and 'regular's } ensure that { when { the EUT det between the	Association established between secure traffic flowing between to tects the expiry of the lifetime e EUT and QE1 } d QE1 are able to communicate se Security Policy defined such that: a. The EUT will accept only secure b. QE1 will accept only secure con c. Security Associations established	he EUT and QE1' of the Security_Ass curely } re communication from mmunication from the J	QE1 EUT	20 s	
Step	Test Se	equence		Ver	dict
				Pass	Fail
1	Preamble: Cause the EUT to send an	1 1			
2	Preamble: Check: Does the EUT rece	eive an Echo Reply fror	n QE1?	Yes	No
3	Cause the EUT to send repeated Eche	o Requests to QE1 for 3	30 seconds		
4	Cause the EUT to send an Echo Requ	uest to QE1			
5	Check: Does the EUT receive an Ech	o Reply from QE1?		Yes	No
Observations:	Step 1 leads to SA establishment betw Untestable By IOP means	ween EUT and QE1			

#### Group 2.3.2: Security Association Lifetime

### Group 2.3.3: Traffic Selector Negotiation

	Test Description						
Identifier:	TD_SEC_6121_01	Test Purpose:	TP_SEC_61	21_01			
Summary:	'A Security Association is created by	A Security Association is created by an IKE endpoint if data is received from a host that is					
	recognized as protected'						
Roles:	Host	<b>Configuration:</b>	CF_SEC_01				
References:	RQ_002_6121						
	gured 'with no Security Associat						
and EUT config	gured ' to recognize QE1 as prot	ected (in its SPD)'					
} ensure that {							
	eives a packet from QE1 }						
	Association is established between	en the EUT and OE1 }					
}		~ ,					
Pre-test conditions:	Security Policy defined such that:						
	a. The EUT will accept only secur	re communication from (	QE1				
	b. QE1 will accept both secure and	d non-secure communica	ation from the I	EUT			
Step	Test Se	equence		Verdict			
				Pass	Fail		
1	Cause QE1 to send an Echo Request	to the EUT					
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No		
3	Cause the EUT to send an Echo Requ	lest to QE1					
4	Check: Does the EUT receive an Ech	o Reply from QE1?		Yes	No		
Observations:		•					

Group 2.4: NAT Traversal

	Test Descr	iption			
Identifier:	TD_SEC_6206_01	Test Purpose:	TP_SEC_62	06_01	
Summary:	'An IKE endpoint accepts messages v	with any UDP Source port	,		
Roles:	Host, Host	Configuration:	CF_SEC_02	4	
References:	RQ_002_6206, RQ_002_6131, RQ_0	002_6206, RQ_002_6212			
and QE2 configure and QE3 configure and QE4 configure } ensure that { when { a Security_	onfigured 'only to communicate securely with QE2' onfigured 'on to communicate securely with the EUT' onfigured 'to translate UDP Source Port numbers for NAT traversal' onfigured 'to translate UDP Source Port numbers for NAT traversal' ecurity_Association is established between the EUT and QE2 } and QE2 are able to communicate securely }				
Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secur b. QE2 will accept only secure con QE3 is configured to translate UDP S QE4 is configured to translate UDP S	mmunications from the El Source Port numbers for N	UT AT traversal		
Step		quence		Vere	lict
-		•		Pass	Fail
1	Cause QE2 to send Traceroute to the	EUT			
2	Check: Does QE2 receive a Tracerou was reached?	te response indicating that	t the EUT	Yes	No
Observations:					

	Test Descr	iption					
Identifier:	TD_SEC_6212_01	Test Purpose:	TP_SEC_62	12_01			
Summary:	'An IKE endpoint sets UDP Destinati	An IKE endpoint sets UDP Destination Port number in IKE responses to the UDP Source Port					
	number from the associated IKE requ	iest'					
Roles:	Host	<b>Configuration:</b>	CF_SEC_02				
References:	RQ_002_6212						
and QE2 configure and QE3 configure and QE4 configure } ensure that { when { a Security_	ed 'only to communicate securely ed 'on to communicate securely w ed 'to translate UDP Source Port ed 'to translate UDP Source Port Association is established betwe 2 are able to communicate secure	ith the EUT' numbers for NAT trave numbers for NAT trave een the EUT and QE2 }					
Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secure b. QE2 will accept only secure con QE3 is configured to translate UDP S QE4 is configured to translate UDP S	mmunications from the El Source Port numbers for N	UT IAT traversal				
Step		quence		Ver	dict		
-		•		Pass	Fail		
1	Cause QE2 to send a Traceroutet to E establishment of a Security Association		Г)				
2	Check: Does QE2 receive a Tracerou was reached?	te response indicating tha	t the EUT	Yes	No		
Observations:							

	Test Des	cription			
Identifier:	TD_SEC_6213_01	Test Purpose:	TP_SEC_6	213_01	
Summary:	'An IKE endpoint sets IPv6 Destina	ation Address in IKE res			Address
•	from the associated IKE request'		-		
Roles:	Host	<b>Configuration:</b>	CF_SEC_0	2	
References:	RQ_002_6213				
	red 'only to communicate secure				
	red 'on to communicate securely				
	red 'to translate IPv6 Source A				
and QE4 configu	red 'to translate IPv6 Source A	ddresses for NAT tra	versal'		
}					
ensure that { when { a Security		ween the sum and OF	2 ]		
	22 are able to communicate secu:		2 }		
}					
Pre-test conditions:	Security Policy defined such that:				
	a. The EUT will accept only see	cure communications from	om QE2		
	b. QE2 will accept only secure of				
	QE3 is configured to translate IPv6				
	QE4 is configured to translate IPv6				
Step		Sequence		Ver	dict
~F		~ • 1 • • • • •		Pass	Fail
1	Cause QE2 to send an Echo Reque	st to EUT (which leads	to the		
	establishment of a Security Association				
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_60	31_01			
Summary:	'An IKE endpoint is able to identify a	nd process a received res			request'		
Roles:	Host	Configuration:	CF_SEC_04	-			
References:	RQ_002_6031						
<pre>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>							
Pre-test conditions:	Security Policy defined such that: a. The EUT will accept only secu b. The EUT will accept only secur c. QE1 will accept only secure co d. QE6 will accept only secure co	e communications from mmunications from the E	QE6 CUT				
Step	Test Se			Ver	dict		
•		•		Pass	Fail		
1	Preamble: Cause QE6 to send unlimit EUT	ted, repeated Echo Reque	sts to the				
2	Cause EUT to send an Echo Request Association establishment)	to QE1 (which leads to S	ecurity				
3	Check: does EUT receive an Echo Re	eply from QE1?		Yes	No		
4	Postamble: Cause QE6 to cease sendi	ng Echo Requests to the	EUT				
<b>Observations:</b>	Untestable by IOP						

	Test Description							
Identifier:	TD_SEC_1020_01	Test Purpose:	TP_SEC_10	20_01				
Summary:	'IPsec Host support of ESP transport							
Roles:	Ipsec_host	Configuration:	CF_SEC_01					
References:	RQ_002_1020, RQ_002_3039							
with { EUT config	gured 'to protect all traffic to	from QE1 using ESP						
	with the transport mode'							
and QE1 conf	igured 'to protect all traffic t	co/from EUT using ESP						
1	with the transport mode'							
ensure that								
{ when { a Securi	ty_Association is established be	etween EUT and QE1 }						
then { QE1 is a	able to communicate with EUT }							
}								
Pre-test conditions:	Security Policy defined such that:							
	a. The EUT will use ESP in Trans	port Mode to secure all co	ommunication	ns to and fi	rom			
	QE1							
	b. QE1 will use ESP in Transport	Mode to secure all comm	unications to	and from t	the EUT			
	Security Association established from	n the EUT to OE1						
	Security Association established from	-						
Step	Test Sequence Verdict							
		-		Pass	Fail			
1	Cause QE1 to establish a Security ass	ociation with EUT						
2	Check: Does QE1 receive an Echo Re	eply from the EUT?		Yes	No			
<b>Observations:</b>					•			

	Test Desc	ription			
Identifier:	TD_SEC_1020_02	Test Purpose:	TP_SEC_10	20_02	
Summary:	'IPsec Host support of AH transport	mode'			
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01		
References:	RQ_002_1020, RQ_002_3039	·	-		
and QE1 conf } ensure that { when { a Securi	<pre>gured 'to protect all traffic to with the transport mode' igured 'to protect all traffic with the transport mode' ty_Association is established hable to communicate with EUT } Security Policy defined such that: a. The EUT will use AH in Transport b. QE1 will use AH in Transport Security Association established from Security Association established from</pre>	to/from EUT using AH between EUT and QE1 } port Mode to secure all common n the EUT to QE1			-
Step		equence		Vero	lict
Step		equence		Pass	Fail
1	Cause QE1 to send an Echo Request	to the EUT			
2	Check: Does QE1 receive an Echo R	eply from the EUT?		Yes	No
Observations:					

	Test Descr	iption			
Identifier:	TD_SEC_1023_01	Test Purpose:	TP_SEC_10	023_01	
Summary:	'IPsec Gateway Support of ESP trans		• <u> </u>		
Roles:	Ipsec_gateway	Configuration:	CF_SEC_03	3	
References:	RQ_002_1023, RQ_002_3039				
and QE4 config ensure that { when { a Secur	<pre>gured 'to protect all traffic to with the transport mode' gured 'to protect all traffic to with the transport mode' city_Association is established : d QE2 are able to communicate }</pre>	/from EUT using ESP }			
} Pre-test conditions:	<ul> <li>Security Policy defined such that:</li> <li>a. The EUT will use ESP in Trans QE4</li> <li>b. QE4 will use ESP in Transport</li> <li>Security Association established from</li> <li>Security Association established from</li> </ul>	Mode to secure all comm n QE4 to EUT			
Step	Test Se	equence		Vere	lict
•		-		Pass	Fail
1	Cause QE1 to send an Echo Request	to QE2			
2	Check: Does QE1 receive an Echo R	eply from QE2?		Yes	No
<b>Observations:</b>					

	Test Desc	ription			
Identifier:	TD_SEC_1023_02	Test Purpose:	TP_SEC_10	023_02	
Summary:	'IPsec Gateway Support of AH trans	port mode'			
Roles:	Ipsec_gateway	<b>Configuration:</b>	CF_SEC_03	3	
References:	RQ_002_1023, RQ_002_3039				
	gured 'to protect all traffic to with the transport mode' gured 'to protect all traffic to with the transport mode'	_			
	rity_Association is established d QE2 are able to communicate }	between EUT and QE4	}		
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 S	equence		Verd	lict
-		-		Pass	Fail
1	Cause QE1 to send an Echo Request	t to QE2			
2	Check: Does QE1 receive an Echo F	Reply from QE2?		Yes	No
<b>Observations:</b>					

	Test Description								
Identifier:	TD_SEC_1021_01	Test Purpose:	TP_SEC_10	021_01					
Summary:	'IPsec Host support of ESP tunnel mo	ode'							
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	l					
References:	RQ_002_1021, RQ_002_3040								
and QE1 conf } ensure that	<pre>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' }</pre>								
	urity_Association is established s able to communicate with EUT		J						
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 Se	quence		Vere	lict				
-		-		Pass	Fail				
1	Cause QE1 to send an Echo Request	to EUT							
2	Check: Does QE1 receive an Echo Ro	eply from the EUT?		Yes	No				
<b>Observations:</b>				•	•				

	Test Descr	iption			
Identifier:	TD_SEC_1021_02	Test Purpose:	TP_SEC_10	21_02	
Summary:	'IPsec Host support of AH tunnel mo	de'	•		
Roles:	Ipsec_host	Configuration:	CF_SEC_01		
References:	RQ_002_1021, RQ_002_3040				
and QE1 cons } ensure that { when { a Sec	gured 'to protect all traffic to with the tunnel mode' Eigured 'to protect all traffic with the tunnel mode' curity_Association is establishe is able to communicate with EUT Security Policy defined such that:	to/from EUT using AH d between EUT and QE1 }			
	<ul> <li>a. The EUT will use AH in Tunnel Mode to secure all communications to and from QE1</li> <li>b. QE1 will use AH in Tunnel Mode to secure all communications to and from the EUT</li> <li>Security Association established from the EUT to QE1</li> <li>Security Association established from QE1 to the EUT</li> </ul>				
Step	Test Se	equence		Ver	dict
-		-		Pass	Fail
1	Cause QE1 to send an Echo Request	to the EUT			
2	Check: Does QE1 receive an Echo R	eply from the EUT		Yes	No
<b>Observations:</b>					·

	Test Description						
Identifier:	TD_SEC_1022_01	Test Purpose:	TP_SEC_10	22_01			
Summary:	'IPsec Gateway support of ESP tunn	el mode'	-				
Roles:	Ipsec_gateway	<b>Configuration:</b>	CF_SEC_03	3			
References:	RQ_002_1022, RQ_002_3040						
and QE4 config } ensure that { when { a Secur	<pre>gured 'to protect all traffic to with the tunnel mode' gured 'to protect all traffic to with the tunnel mode' rity_Association is established d QE2 are able to communicate }</pre>	o/from EUT using ESP					
Pre-test conditions:	Security Policy defined such that: a. The EUT will use ESP in Tunr b. QE4 will use ESP in Tunnel M Security Association established from Security Association established from	ode to secure all commu m QE4 to EUT			-		
Step	Test Sequence Verdict						
~~ <b>··</b> P		- 1		Pass	Fail		
1	Cause QE1 to send an Echo Request	to QE2					
2		eck: Does QE1 receive an Echo Reply from QE2? Yes No					
Observations:		•			•		

	Т	est Description				
Identifier:	TD_SEC_1022_02	Test Purpose:	TP_SEC_10	022_02		
Summary:	'IPsec Gateway support of A	AH tunnel mode'				
Roles:	Ipsec_gateway	Configuration:	CF_SEC_0	3		
References:	RQ_002_1022, RQ_002_30					
,	with the tunnel m	affic to/from EUT using AH				
	nd QE2 are able to commun		1 }			
Pre-test conditions:	<ul><li>b. QE4 will use AH in T</li><li>c. QE1 will only accept</li></ul>	I in Tunnel Mode to secure all c 'unnel Mode to secure all comm secure communication from QE secure communication from QE ished from QE2 to QE1	unications to and 22		-	
Step		Test Sequence		Ver	dict	
				Pass	Fail	
1	Cause QE1 to send an Echo	Request to QE2				
2	Check: Does QE1 receive a	heck: Does QE1 receive an Echo Reply from QE2? Yes No				
<b>Observations:</b>						

	1	<b>Test Description</b>			
Identifier:	TD_SEC_3000_01	Test Purpose:	TP_SEC_30	00_01	
Summary:	'IPsec host supports integri	ty-only ESP'	<u>.</u>		
Roles:	Ipsec_host	Configuration:	CF_SEC_01		
References:	RQ_002_3000				
and QE1 } ensure that { when { EUT	nfigured 'to protect commun the integrity s configured 'to accept only the integrity s receives a packet from QE1 indicating that a response indicates receipt of the re	service of ESP' packets protected using onl service of ESP' is requested }			
Pre-test conditions	<ul><li>a. EUT will protect com</li><li>b. QE1 will accept only</li></ul>	th that: munication with QE1 using only packets protected by the integrists sts between the EUT and QE1 (1	ity service of ESI		SP
Step         Test Sequence         Ve					
•		*		Pass	Fail
1	Cause QE1 to send an Echo	o Request to EUT			
2	Check: does QE1 receive a	n Echo Reply from the EUT?		Yes	No
Observations:					

	Test Descr	iption			
Identifier:	TD_SEC_3001_01	<b>Test Purpose:</b>	TP_SEC_30	01_01	
Summary:	'IPsec host supports full-service ESP'				
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01		
References:	RQ_002_3001				
and QE1 conf } ensure that { when { EUT rece ind:	<pre>gured 'to protect communication ' using the confidentiali services of ESP' Eigured 'to accept only packets ; using the confidentiali services of ESP' eives a packet from QE1 leating that a response is reque leates receipt of the response }</pre>	ty and integrity protected ty and integrity			
Pre-test conditions:	<ul> <li>Security Policy defined such that:</li> <li>a. EUT will protect communication services of ESP</li> <li>b. QE1 will accept only packets press</li> <li>A Security Association exists between</li> </ul>	rotected by the confide	entiality and inte	U	•
Step Test Sequence Ver					lict
				Pass	Fail
1	Cause QE1 to send an Echo Request	to EUT			
2	Check: does QE1 receive an Echo Re	ply?		Yes	No
Observations:					

	Tes	t Description			
Identifier:	TD_SEC_3002_01	Test Purpose:	TP_SEC_30	02_01	
Summary:	'IPsec host supports confident	tiality-only ESP'	·		
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01		
References:	RQ_002_3002 gured 'to protect communic				
<pre>} ensure that {    when { EUT rec         ind         then { QE1 ind    } }</pre>	figured 'to accept only pa	<pre>nfidentiality service of requested }</pre>			
Pre-test conditions:	-	unication with QE1 using onluckets protected by the confid	lentiality service	•	e of ESP
Step Test Sequence Vero					
				Pass	Fail
1	Cause QE1 to send an Echo R	Request to EUT			
2	Check: does QE1 receive an H	Echo Reply?		Yes	No
Observations:					

	Test Description					
Identifier:	TD_SEC_3013_01	D_SEC_3013_01 <b>Test Purpose:</b> TP_SEC_3013_01				
Summary:	'IPsec host does not increment the s	equence number to a value	greater than the	biggest (	32-bit	
	number'					
Roles:	Ipsec_host	Configuration:	CF_SEC_01			
References:	RQ_002_3013					
and EUT configu and QE1 configu and QE1 configu and a Security_ } ensure that { when { EUT is r greated then { EUT and EUT }	red 'to use ESP to secure its red 'to activate anti-replay' red 'to use ESP to secure its red 'to activate anti-replay' Association established betwee requested to send a packet cont ater than 'the biggest 32-bit deletes the established Securi establishes a new Security_Ass	communication with EUT en the EUT and QE1 caining a sequence_numb number' } .ty_Association to QE1 sociation to QE1 }	,			
Pre-test conditions:	NOT TESTABLE BY INTEROPE					
	This would imply sending more than 4 000 000 packets					
Step	Test	Sequence	-	Verd		
				Pass	Fail	
<b>Observations:</b>						

	Т	est Description			
Identifier:	TD_SEC_3054_01	Test Purpose:	TP_SEC_30	)54_01	
Summary:	'IPsec host maintains the see	quence number ESP Security A	Associations acros	ss local reb	oots
-	when anti-replay is activate	d'			
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	1	
References:	RQ_002_3054				
and EUT co and QE1 co and QE1 co and an ESI betwee } ensure that { when { EUT is then { QE1 is }	Figured 'to activate anti- onfigured 'to protect its o onfigured 'to activate anti- onfigured 'to protect its o P Security_Association esta- en the EUT and QE1 s requested to reboot } s able to communicate with	communication with QE1 usi i-replay' communication with EUT usi ablished EUT after the reboot }			
Pre-test conditions:	b. QE1 will use ESP to p EUT is configured to activa QE1 is configured to activat	P to protect all of its communic protect all of its communication te anti-replay	as with the EUT	lirections)	
Step		Test Sequence		Ver	dict
				Pass	Fail
1	Cause the EUT to send 10 E	Echo Requests to QE1			
2	Reboot the EUT				
3	Cause QE1 to send an Echo	Request to EUT			
4	Check: does QE1 receive ar	Echo Reply from EUT?		Yes	No
Observations:					

	Tes	t Description			
Identifier:	TD_SEC_3061_01	Test Purpose:	TP_SEC_30	)61_01	
Summary:	'IPsec host discards any packe	et containing an ESP Header th	at does not mat	ch any Sec	curity
	Association'				
Roles:	Ipsec_host, Ipsec_host	<b>Configuration:</b>	CF_SEC_0	1	
References:	RQ_002_3061, RQ_002_306	1, RQ_002_3091			
and QE1 con } ensure that { when { EUT rec conta indic then { EUT dis	t having established any S figured 'to use ESP to sec eives a packet from QE1 ining an ESP_Header ating that a response is r cards the packet ds no response to QE1 }	ure its communication with			
Pre-test conditions:	b. QE1 will use ESP to pro	hat: o protect all of its communicat otect all of its communications tablished between the EUT and	with the EUT		
Step		Test Sequence	· <b>`</b>	Ver	dict
*		*		Pass	Fail
1	Cause QE1 to send an Echo R	lequest to EUT			
2	Check: does QE1 receive an H	*		No	Yes
<b>Observations:</b>					

	Test Desc	ription	
Identifier:	TD_SEC_3063_01	Test Purpose:	TP_SEC_3063_01
Summary:	'IPsec host supports anti-replay servi		·
Roles:	Ipsec_host	Configuration:	CF_SEC_01
References:	RQ_002_3063, RQ_002_3068, RQ_		
<pre>and EUT config and QE1 config and QE1 config } ensure that { when { EUT rec cor in then { EUT ser } Pre-test conditions:</pre>	<ul> <li>the ESP integrity only service</li> <li>e. QE1 will only accept communintegrity only service</li> <li>f. QE6 will only accept communintegrity only service</li> <li>EUT is configured to enable anti-rep</li> <li>QE1 is configured to enable anti-rep</li> <li>QE6 is configured to enable anti-</li></ul>	on with QE1' of ESP on with EUT' nce_number unications to QE1 and QE4 ations to the EUT using the ations to the EUT using the ations to the EUT using the munications from QE1 and ications from the EUT if th ications from the EUT if th blay lay k-local address as QE1 blished between the EUT a blished between the EUT a blished between the EUT a	e ESP integrity only service ESP integrity only service d QE6 if they are secured using ney are secured using the ESP ney are secured using the ESP
Step	l lest 5	equence	Pass Fail
1	Cause QE6 to send an Echo Request	to EUT	
2	Check: does QE6 receive an Echo R		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 R		No Yes
Observations:		* *	

	Test Description				
Identifier:	TD_SEC_3064_01 Test Pu	rpose:	TP_SEC_30	64_01	
Summary:	'IPsec host does not enable anti-replay service	when integrity	service is not e	enabled for	r the
	Security Association'				
Roles:	Ipsec_host Configu	uration:	CF_SEC_01		
References:	RQ_002_3064				
<pre>and EUT configu and QE1 configu and QE1 configu and a Security_ } ensure that { when { EUT rece cont and indi</pre>	red 'to use ESP to secure its communicated red 'with the integrity service disables red 'to use ESP to secure its communicated red 'with the integrity service disables Association established between the EUT ives a packet from QE1 aining a previously used sequence_number in the Authentication_Header cating that a response is requested } cates receipt of the response } Security Policy defined such that: a. The EUT will secure all communication integrity only service b. QE1 will secure all communications to the service c. QE6 will secure all communications to the service d. The EUT will only accept communications f. QE6 will only accept communications for 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 and QE1 is disconnected from Network A security association has been established be parameters to those set for the SA between the <b>Test Sequence</b>	ed' ation with EU ed' r and QE1 er s to QE1 and Q he EUT using H he EUT using H he EUT using H ons from QE1ar rom the EUT if rom the EUT if dress as QE1 etween the EUT tween the EUT	DE6 using ESP to ESP but not the ESP but not the nd QE6 if they if they are secure they are secure T and QE1 T and QE6 using	integrity of integrity of are secured are secured are using ES	only only d using SP S
1				Pass	Fail
1	Cause QE6 to send an Echo Request to EUT	EUT9		Ver	N-
2	Check: does QE6 receive an Echo Reply from	EUI!		Yes	No
3 4	Disconnect QE6 from Network B				
4	Connect QE1 to Network B				
	Cause OE1 to see J on E-1 D to set ( DUT				
5	Cause QE1 to send an Echo Request to EUT Check: does QE1 receive an Echo Reply from			Yes	No

	T	est Description			
Identifier:	TD_SEC_3065_01	Test Purpose:	TP_SEC_30	65_01	
Summary:	'IPsec host does not check S	equence Number on Multisen	der ESP Security A	Associatio	ns'
Roles:	Ipsec_host	Configuration:	CF_SEC_01		
References:	RQ_002_3065				
and QE1 confi and a Multise between t } ensure that { when { EUT re co and ir		re its communication with established d sequence_number ation_Header is requested } sponse }	EUT'		
		mmunication with EUT using ociation has been established been established between the senders)		as the rec	ipient)
Step		Test Sequence		Vere	lict
_		_		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			Yes	No
Observations:		- ·			

		Test Description	
Identifier:	TD_SEC_2014_01	Test Purpose:	TP_SEC_2014_01
Summary:	'IPsec host does not in number'	crement the sequence number to a val	ue greater than the biggest 32-bit
Roles:	Ipsec_host	Configuration:	CF_SEC_01
References:	RQ_002_2014		
and EUT c and QE1 c and QE1 c and a Sec } ensure that { when { EUT i then { E and E }	its communi configured 'to activate configured 'to use Auth its communi configured 'to activate curity_Association esta .s requested to send a greater than 'the bigg CUT deletes the establi	entication Header to secure cation with EUT' anti-replay' blished between the EUT and QE1 packet containing a sequence_nu	mber
Pre-test conditions:		INTEROPERABILITY MEANS	
~	This would imply send	ling more than 4 000 000 000 packets	
Step		Test Sequence	Verdict
			Pass Fail
Observations:			

	Test I	Description		
Identifier:	TD_SEC_2046_01	Test Purpose:	TP_SEC_2046_01	
Summary:	'IPsec host discards any packet c	ontaining an Authentication	on Header that does not mate	ch any
	Security Association'			
Roles:	Ipsec_host, Ipsec_host	<b>Configuration:</b>	CF_SEC_01	
References: with { EUT confid	RQ_002_2046, RQ_002_2046 gured 'to use Authentication			
and QE1 conf } ensure that { when { EUT rece conta: indice then { EUT disc	its communication w t having established any Sec figured 'to use Authentication its communication w eives a packet from QE1 ining an Authentication_Head ating that a response is req cards the packet ds no response to QE1 }	urity Association with on Header to secure ith EUT' er	. QEl'	
Pre-test conditions:	<ul> <li>Security Policy defined such tha</li> <li>a. The EUT will use AH to secure</li> <li>b. QE1 will use AH to secure</li> <li>c. Security Associations between needed</li> </ul>	ecure all of its communica all of its communications ween the EUT and QE1 will	with the EUT Il not be created automatical	ly when
Step	Test Sequence		Verd	lict
~			Pass	Fail
1	Cause QE1 to send an Echo Req	uest to EUT		
2	Check: does QE1 receive an Ech		No	Yes
Observations:		1 V		

	Te	est Description					
Identifier:	TD_SEC_2057_01	Test Purpose:	TP_SEC_2	057_01			
Summary:	'IPsec host calculates Integr	Psec 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	<b>Configuration:</b>	CF_SEC_0	1			
References:	RQ_002_2057, RQ_002_20	28, RQ_002_2057					
and QE1 conf and a Sec } ensure that { when { QE1 s cont indi	igured 'to use Authenticati its communication w igured 'to use Authenticati its communication w urity_Association establish ends a packet to EUT aining an Authentication_He cating that a response is n ndicates receipt of the res	with QE1' Ion Header to secure with EUT' hed between the EUT and QE eader requested }	1				
Pre-test conditions:	b. QE1 will use AH to se The EUT has established a	n that: to secure all of its communica cure all of its communications Security Association with QE ity Association with the EUT	with the EUT				
Step		Test Sequence		Ver	dict		
				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		
<b>Observations:</b>							

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

	Test Description						
Identifier:	TD_SEC_5002_01	Test Purpose:	TP_SEC_50	02_01			
Summary:	'Support of NULL encryption algorit	hm'					
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01				
References:	RQ_002_5002						
and QE1 conf } ensure that { when { a Securi	gured 'to protect all traffic to with NULL encryption alg Eigured 'to protect all traffic with NULL encryption alg .ty_Association is established b the EUT are able to communicate	orithm' to/from EUT using ESP orithm' etween EUT and QE1 }					
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 Se	equence		Vero	lict		
				Pass	Fail		
1	Cause QE1 to send an Echo Request	to EUT					
2	Check: does QE1 receive an Echo Re	eply from the EUT?		Yes	No		
<b>Observations:</b>							

	Test Description							
Identifier:	TD_SEC_5003_01	Test Purpose:	TP_SEC_50	03_01				
Summary:	'Supports of TripleDES-CBC encrypt	ion algorithm'						
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01					
References:	RQ_002_5003							
<pre>with { EUT configured 'to protect all traffic to/from QE1 using ESP</pre>								
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 Se	quence		Vero	lict			
-		_		Pass	Fail			
1	Cause QE1 to send an Echo Request	to EUT						
2	Check: does QE1 receive an Echo Re	ply from the EUT?		Yes	No			
Observations:								

	Test Desci	ription			
Identifier:	TD_SEC_5004_01	Test Purpose:	TP_SEC_50	04_01	
Summary:	'Support of AES-CBC encryption alg	gorithm with 128-bit key	length'		
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	-	
References:	RQ_002_5004				
and QE1 conf } ensure that { when { a Securi	<pre>gured 'to protect all traffic to with AES-CBC encryption figured 'to protect all traffic with AES-CBC encryption 128-bit key length' .ty_Association is established h the EUT are able to communicate Security Policy is defined such that: a The EUT will protect all traffic</pre>	algorithm and with 12 to/from EUT using ESF algorithm and with etween EUT and QE1 } }			
	<ul> <li>a. The EUT will protect all traffic to/from QE1 using ESP with ES-CBC encryption algorithm with 128-bit key length</li> <li>b. QE1 will protect all traffic to/from the EUT using ESP with ES-CBC encryption algorithm with 128-bit key length</li> <li>A Security Association is established between the EUT and QE1 (both directions)</li> </ul>				
Step	Test Se	equence		Verd	lict
				Pass	Fail
1	Cause QE1 to send an Echo Request				
2	Check: does QE1 receive an Echo Re	eply from the EUT?		Yes	No
Observations:					

	Test Desc	ription				
Identifier:	TD_SEC_5005_01	Test Purpose:	TP_SEC_50	005_01		
Summary:	'Support of AES-CTR encryption alg	gorithm'	-			
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	1		
References:	RQ_002_5005					
and QE1 con } ensure that { when { a Secu:	igured 'to protect all traffic to with AES-CTR encryption hfigured 'to protect all traffic with AES-CTR encryption rity_Association is established h d the EUT are able to communicate Security Policy is defined such that: a. The EUT will protect all traffic algorithm	algorithm' to/from EUT using algorithm' petween EUT and QE1 e } c to/from QE1 using E	ESP } CSP with AES-CT	• •		
	<ul> <li>b. QE1 will protect all traffic to/from the EUT using ESP with AES-CTR encryption algorithm</li> <li>A Security Association is established between the EUT and QE1 (both directions)</li> </ul>					
Step		equence		Ver	dict	
•		-		Pass	Fail	
1	Cause QE1 to send an Echo Request	to EUT				
2	Check: does QE1 receive an Echo R			Yes	No	
Observations:	~	* *		•	•	

	Test Descr	iption			
Identifier:	TD_SEC_5007_01	Test Purpose:	TP_SEC_50	007_01	
Summary:	'Support of HMAC-SHA1 authentica	tion algorithm'			
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	l	
References:	RQ_002_5007				
and QE1 con } ensure that { when { a Secur	gured 'to protect all traffic to with HMAC-SHA1 authentic figured 'to protect all traffic with HMAC-SHA1 authentic ity_Association is established b the EUT are able to communicate	ation algorithm' to/from EUT using ESF ation algorithm' etween EUT and QE1 }	•		
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 Se	quence		Ver	dict
		-		Pass	Fail
1	Cause QE1 to send an Echo Request	to EUT			
2	Check: does QE1 receive an Echo Re	ply from the EUT?		Yes	No
<b>Observations:</b>					

	Test Description							
Identifier:	TD_SEC_5008_01	Test Purpose:	TP_SEC_50	008_01				
Summary:	'Support of NULL authentication alg	orithm'						
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	l				
References:	RQ_002_5008							
} ensure that { when { a Secur	with NULL authentication figured 'to protect all traffic with NULL authentication rity_Association is established b d the EUT are able to communicate Security Policy is defined such that:	to/from EUT using H algorithm' petween EUT and QE1						
<ul> <li>a. The EUT will protect all traffic to/from QE1 using ESP with NULL authentication algorithm</li> <li>b. QE1 will protect all traffic to/from the EUT using ESP with NULL authentication algorithm</li> <li>A Security Association is established between the EUT and QE1 (both directions)</li> </ul>								
Step	Test Se	equence		Ver	lict			
-		-		Pass	Fail			
1	Cause QE1 to send an Echo Request	to EUT						
2	Check: does QE1 receive an Echo Re	eply from the EUT?		Yes	No			
<b>Observations:</b>								

	Test Description							
Identifier:	TD_SEC_5009_01	Test Purpose:	TP_SEC_50	09_01				
Summary:	'Support of AES-XCBC-MAC auther	ntication algorithm'						
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01	l				
References:	RQ_002_5009							
} ensure that { when { a Secur then { QE1 and }	with AES-XCBC-MAC authen figured 'to protect all traffic with AES-XCBC-MAC authen ity_Association is established b the EUT are able to communicate	to/from EUT using E tication algorithm' etween EUT and QE1						
<ul> <li>Pre-test conditions: Security Policy is defined such that:</li> <li>a. The EUT will protect all traffic to/from QE1 using ESP with AES-XCBC-MAC-96 authentication algorithm</li> <li>b. QE1 will protect all traffic to/from the EUT using ESP with AES-XCBC-MAC-96 authentication algorithm</li> <li>A Security Association is established between the EUT and QE1 (both directions)</li> </ul>								
Step	Test Se	equence		Ver	dict			
_				Pass	Fail			
1	Cause QE1 to send an Echo Request	to EUT						
2	Check: does QE1 receive an Echo Re	eply from the EUT?		Yes	No			
Observations:								

Test Description							
Identifier:	TD_SEC_5010_01	Test Purpose:	TP_SEC_50	10_01			
Summary:	'Support of HMAC-MD5 authentication	on algorithm'	•				
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01				
References:	RQ_002_5010						
and QE1 coni } ensure that { when { a Secur:	gured 'to protect all traffic to with HMAC-MD5 authentica Figured 'to protect all traffic with HMAC-MD5 authentica ty_Association is established bo the EUT are able to communicate	tion algorithm' to/from QE1 using ESP tion algorithm' etween EUT and QE1 }					
<ul> <li>Pre-test conditions: Security Policy is defined such that:</li> <li>a. The EUT will protect all traffic to/from QE1 using ESP with HMAC-MD5 authentication algorithm</li> <li>b. QE1 will protect all traffic to/from the EUT using ESP with HMAC-MD5 authentication algorithm</li> <li>A Security Association is established between the EUT and QE1 (both directions)</li> </ul>							
Step	Test Se	quence		Vero	lict		
-		-		Pass	Fail		
1	Cause QE1 to send an Echo Request	to EUT					
2	Check: does QE1 receive an Echo Re	ply from the EUT?		Yes	No		
Observations:							

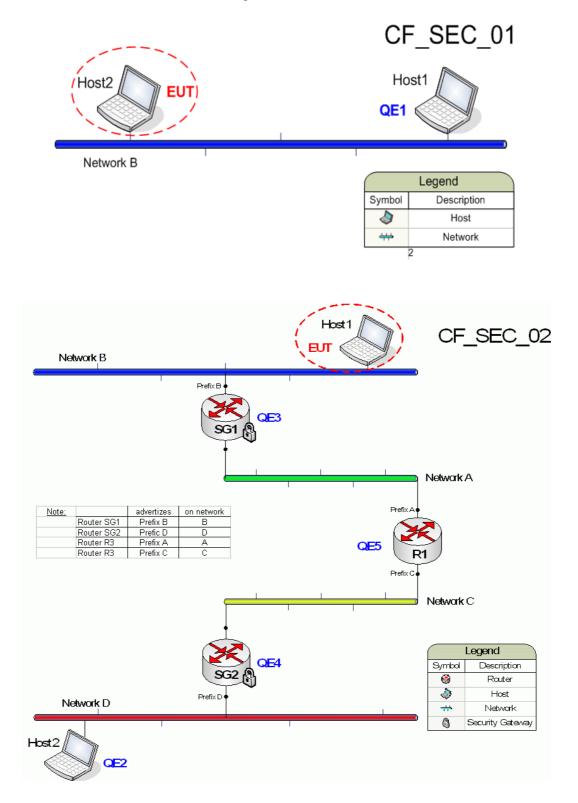
	Test Descr	ription			
Identifier:	TD_SEC_5012_01	Test Purpose:	TP_SEC_50	012_01	
Summary:	'Support of HMAC-SHA1 as authent	ication algorithm for A	H'		
Roles:	Ipsec_host	<b>Configuration:</b>	CF_SEC_01		
References:	RQ_002_5012				
and QE1 conf and QE1 conf } ensure that { when { a Securi	pured 'with HMAC-SHA1 as authent Authentication Header ' Figured 'with HMAC-SHA1 as authe Authentication Header ' Figured 'to accept traffic from/ Cty_Association is established b the EUT are able to communicate	ntication algorithm to EUT only if secur etween EUT and QE1	for red'		
Pre-test conditions:	<ul> <li>Security Policy is defined such that:</li> <li>a. The EUT will protect all traffic authentication algorithm</li> <li>b. QE1 will protect all traffic to/fr algorithm</li> <li>A Security Association is established</li> </ul>	rom the EUT using AH	with HMAC-SI	HA1 authe	ntication
Step		equence		Vero	lict
~~~F		1		Pass	Fail
1	Cause QE1 to send an Echo Request	to EUT			
2	Check: does QE1 receive an Echo Re			Yes	No
Observations:				•	

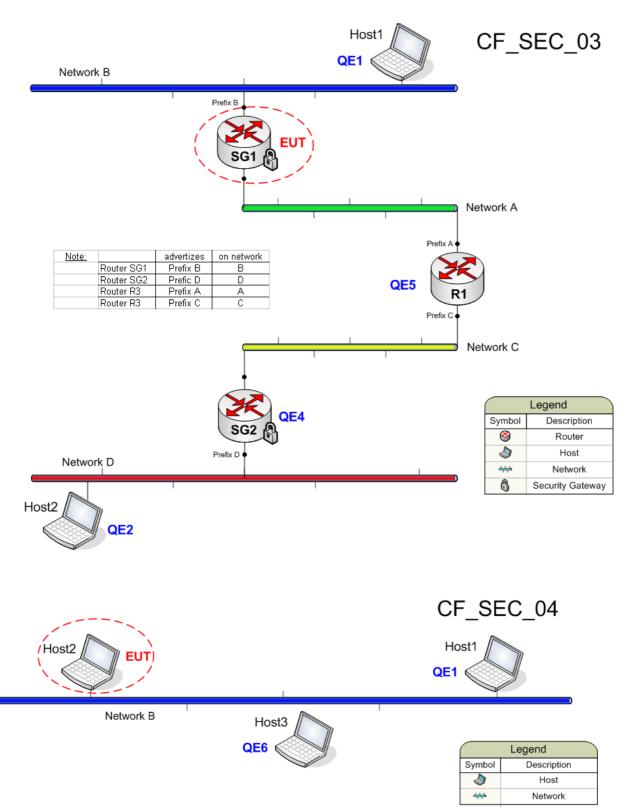
Test Description							
Identifier:	TD_SEC_5013_01 Test Purpose:		TP_SEC_5013_01				
Summary:	'Support of AES-XCBC-MAC as authentication algorithm for AH'						
Roles:	Ipsec_host Configuration: CF_SEC_01						
References:	RQ_002_5013						
<pre>with { EUT configured 'with AES-XCBC-MAC as authentication algorithm</pre>							
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				
···· r		1		Pass	Fail		
1	Cause QE1 to send an Echo Request	to EUT					
2	Check: does QE1 receive an Echo Re	ply from the EUT?		Yes	No		
Observations:							

Test Description						
Identifier:	TD_SEC_5014_01	Test Purpose:				
Summary:	Support of HMAC-MAC as authentication algorithm for AH'					
Roles:	Ipsec_host	Configuration:	CF_SEC_01			
References:	RQ_002_5014					
<pre>with { EUT configured 'with HMAC-MAC as authentication algorithm for</pre>						
	 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.





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
       : 'IPv6 Security Test Purposes'
Title
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 EUT configured 'to accept traffic from QE1 only if secured' with { 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

41

using that security_association}

}

--xxxxxxxxxxxxxxxxxxxxxxxx **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 EUT configured 'to accept traffic only if secured' and QE1 'having successfully established a single IKE SA with EUT' with { 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 } } --xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx : TP SEC 6041 01 TP id 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 EUT configured 'only to communicate securely with QE1' with { 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 --xxxxxxxxxxxxxxxxxxxxxxxxxxx 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 : IPsec_host Role 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 EUT configured 'to support certificate authentication' with { 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 }

} --xxxxxxxxxxxxxxxxxxxxxxxxxxx **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 } { EUT and QE1 are able to communicate securely } then } End Group 2.2 --xxxxxxxxxxxxxxxxxxxxxxxxxx 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 : Host Role 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 } } --xxxxxxxxxxxxxxxxxxxxxxxxxxx **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
        : Host
Role
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
--xxxxxxxxxxxxxxxxxxxxxxxxxxx
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 }
        { EUT and QE2 are able to communicate securely }
  then
          }
 -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 {\tt 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 }
        { EUT and QE2 are able to communicate securely }
  then
         }
--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 \widetilde{\text{QE4}} configured 'to translate IPv6 Source Addresses for NAT traversal'
      }
ensure that {
  when { a Security_Association is established between the EUT and QE2 }
        { EUT and QE2 are able to communicate securely }
  then
          }
End Group 2.4
--xxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
       : Host
Role
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
            EUT configured 'to use ESP to secure its communication with QE1'
  with {
         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 }
    }
 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
         EUT configured 'to activate anti-replay'
and EUT configured 'to protect its communication with QE1 using ESP'
  with {
         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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
            EUT configured 'to protect communication with QE1
  with {
                             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
        : IPsec_Host
Role
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_3000_01
summary : 'IPsec host supports integrity-only ESP'
RQ ref : RQ_002_3000
       : IPsec_Host
Role
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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' }
                 EUT deletes the established Security_Association to QE1
      then {
```

```
and EUT establishes a new Security_Association to QE1 }
    }
 -xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_3064_01
\ensuremath{\textbf{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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
       : IPsec_Host
Role
config : CF_SEC_01
TD ref : TD_SEC_2046_01
  with {
            EUT configured 'to use Authentication Header to secure
```

its communication with OE1'

ETSI

```
49
```

```
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 }
    1
--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
            EUT configured 'to use Authentication Header to secure
  with {
                             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' }
                 EUT deletes the established Security_Association to QE1
      then {
             and EUT establishes a new Security_Association to QE1 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
     : IPsec_Host
Role
config : CF_SEC_01
TD ref : TD_SEC_2057_01
  with
         EUT configured 'to use Authentication Header to secure
   {
                          its communication with OE1'
      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
           EUT configured 'to protect all traffic to/from QE1 using ESP'
  with {
         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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_1020_01
summary : 'IPsec Host support of ESP transport mode'
RQ ref : RQ_002_1020, RQ_002_3039
       : IPsec_Host
Role
config : CF_SEC_01
TD ref : TD_SEC_1020_01
            EUT configured 'to protect all traffic to/from QE1 using ESP
  with {
         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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_1020_02
summary : 'IPsec Host support of AH transport mode'
RQ ref : RQ_002_1020, RQ_002_3039
       : IPsec_Host
Role
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
    \{ \mbox{ when } \{ \mbox{ a Security_Association is established between EUT and QE1 } \}
      then { QE1 is able to communicate with EUT }
    }
```

--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

TP id : TP_SEC_1021_01 summary : 'IPsec Host support of ESP tunnel mode' **RQ ref** : RQ_002_1021, RQ_002_3040 : IPsec_Host Role config : CF_SEC_01 **TD ref** : TD_SEC_1021_01 EUT configured 'to protect all traffic to/from QE1 using ESP with { 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 : IPsec_Host Role 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 } } --xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx TP id : TP_SEC_1022_01 summary : 'IPsec Gateway support of ESP tunnel mode' **RQ ref** : RQ_002_1022, RQ_002_3040 : IPsec_Gateway Role 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 $\{ \mbox{ when } \{ \mbox{ a Security_Association is established between EUT and QE4 } \}$ then { QE1 and QE2 are able to communicate } } --xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx **TP id** : TP_SEC_1022_02 summary : 'IPsec Gateway support of AH tunnel mode' **RQ ref** : RQ_002_1022, RQ_002_3040 : IPsec_Gateway Role 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
     \{ \mbox{ when } \{ \mbox{ a Security_Association is established between EUT and QE4 } \}
       then { QE1 and QE2 are able to communicate }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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 }
     }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_1023_02
summary : 'IPsec Gateway Support of AH transport mode'
RQ ref : RQ_002_1023, RQ_002_3039
        : IPsec_Gateway
Role
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 }
     }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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
             EUT configured 'to protect all traffic to/from QE1 using ESP
  with {
                             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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_5004_01
summary : 'Support of AES-CBC encryption algorithm with 128-bit key length'
RQ ref : RQ_002_5004
        : IPsec Host
Role
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
             EUT configured 'to protect all traffic to/from QE1 using ESP
  with {
                             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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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_SEC_5007_01
TD ref
  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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
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 }
    }
--xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
TP id : TP_SEC_5010_01
summary : 'Support of HMAC-MD5 authentication algorithm'
RQ ref : RQ_002_5010
       : IPsec_Host
Role
config : CF_SEC_01
TD ref : TD_SEC_5010_01
           EUT configured 'to protect all traffic to/from QE1 using ESP
  with {
                           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 }
    }
--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 } } --xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx **TP id** : TP_SEC_5013_01 summary : 'Support of AES-XCBC-MAC as authentication algorithm for AH' **RQ ref** : RQ_002_5013 : IPsec_Host Role 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 } } --xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx **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 } }

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		