IPv6 Ready Logo Phase-2

Interoperability Test Scenario
IKEv2

Technical Document

Revision 1.1.0

IPv6 Forum *http://www.ipv6forum.org/*
IPv6 Ready Logo Committee *http://www.ipv6ready.org/*

MODIFICATION RECORD

Version 1.1.0 Jun. 8, 2010

Major Revision Up Items

- Added IKEv2 Interop.1.4 Part AA, BB, GG, and HH Cryptographic Algorithm Negotiation for IKE_SA using PRF_HMAC_SHA2_256
- Added IKEv2 Interop 1.4 Part CC, DD, II, and JJ Cryptographic Algorithm Negotiation for IKE_SA using AUTH_HMAC_SHA2_256_128
- Added IKEv2 Interop.1.4. Part EE, FF, KK, and LL Cryptographic Algorithm Negotiation for IKE_SA using 2048 MODP Group with 256-bit Prime Order Subgroup
- Added IKEv2 Interop.1.5 Part AA, BB, CC, and DD Cryptographic Algorithm Negotiation for CHILD_SA using AUTH_HMAC_SHA2_256_128
- Updated IKEv2 Interop.1.8 to choose either Diffie-Hellman Group 14 or Diffie-Hellman Group 24
- Updated IKEv2 Interop.1.9 to choose either Diffie-Hellman Group 14 or Diffie-Hellman Group 24

Minor Revision Up Items

- Added configuration file to required data at appendix A
- Updated IKEv2Interop.1.2 and IKEv2Interop.1.3 to be testable regardless of SA life type
- Updated IKEv2Interop.1.8, IKEv2Interop.1.9, IKEv2Interop.1.10 and IKEv2Interop.1.11 to be testable regardless of cryptographic algorithms
- Grouped a default network topology and a default configuration by the usage scenario
- Removed IKEv2 Interop.1.4 Part B, and G Cryptographic Algorithm Negotiation for IKE_SA using ENCR_AES_CTR
- Fixed editorial typos

Version 1.0.1 May 26, 2009

- Corrected Acknowledgment
- Removed IKEv2Interop.1.7 (Identification Type) by mandating to support only ID_IPV6_ADDR
- Updated Requirements, Tests performed on End-Node/SGW according to the removal of IKEv2Interop.1.7

Version 1.0.0 Nov. 28, 2008

- Initial release

ACKNOWLEDGMENTS

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

Authors:

Yokogawa Electric Corporation
Nippon Telegraph and Telephone Corporation (NTT)

Commentators:

NTT Advanced Technology Corporation (NTT-AT)
University of New Hampshire - InterOperability Lab
IRISA-INRIA

Note:

Development of this document was supported in part by a grant from NICT.

INTRODUCTION

Overview

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

Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products.

To avoid confusion in the mind of customers, a globally unique logo programme should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo programme will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase I

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

Phase II

The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Ready Logo Committee (v6RLC).

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

Phase III

Same as Phase 2 with IPsec mandated.

Abbreviations and Acronyms

IKE:	Internet Key Exchange (IKEv2) Protocol
EN:	End-Node
SGW:	Security-Gateway
PSK:	Pre-Shared Key
ESN:	Extended Sequence Numbers
PFS:	Perfect Forward Secrecy
TAR-EN:	Target End-Node
TAR-SGW:	Target Security-Gateway
REF-Host:	Reference Host
REF-Router:	Reference Router

TEST ORGANIZATION

This document organizes tests by Section based on related test methodology or goals. Each group begins with a brief set of comments pertaining to all tests within that group. This is followed by a series of description blocks; each block describes a single test. The format of the description block is as follows:

Test Label: The test label and title comprise the first line of the test block. The test label is composed by concatenating the short test suite name, the section number, the group number, and the test number within the group. These elements are separated by periods. The Test Number is the section, group and test number, also separated by periods.

Purpose: The Purpose is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.

References: The References section lists cross-references to the scenarios and documentation that might be helpful in understanding and evaluating the test and results.

Resource Requirements: The Resource Requirements section specifies the software, hardware, and test equipment that will be needed to perform the test.

Test Setup: The Test Setup section describes the configuration of all devices prior to the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used for that parameter.

Procedure: This section of the test description contains the step-by-step instructions for carrying out the test. These steps include such things as enabling interfaces, unplugging devices from the network, or sending packets from a test station. The test procedure also cues the tester to make observations, which are interpreted in accordance with the observable results given for that test part.

Observable Results: This section lists observable results that can be examined by the tester to verify that the target device is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail for each test is usually based on how the behavior of target device compares to the results described in this section.

Possible Problems: This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

REFERENCES

The following documents are referenced in this text:

[IKEV2] Kaufman, C.,
"Internet Key Exchange (IKEv2) Protocol",
RFC 4306, December 2005.

[RFC4307] Schiller, J.,
"Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)",
RFC 4307, December 2005.

[Clarif] Eronen, P. and P. Hoffman,
"IKEv2 Clarifications and Implementation Guidelines",
RFC 4718, October 2006.

TABLE OF CONTENTS

MODIFICATION RECORD......1

ACKNOWLEDGMENTS......2

INTRODUCTION......3

TEST ORGANIZATION......4

REFERENCES......5

TABLE OF CONTENTS......6

Requirements......8

EQUIPMENT TYPE......8

FUNCTION LIST......8

Tests performed on End-Node/SGW......10

Scenario 1: End-Node to End-Node Transport Mode......12

DEFAULT NETWORK TOPOLOGY 1:......12

DEFAULT CONFIGURATION 1:......13

Default Configuration 1.1: TAR-EN1......13

Default Configuration 1.2: TAR-EN2......14

Scenario 2: SGW to SGW Tunnel Mode......15

DEFAULT NETWORK TOPOLOGY 2:......15

DEFAULT CONFIGURATION 2:......16

Default Configuration 2.1: TAR-SGW1......16

Default Configuration 2.2: TAR-SGW2......17

Scenario 3: End-Node to SGW/SGW to End-Node Tunnel Mode......18

DEFAULT NETWORK TOPOLOGY 3:......18

DEFAULT CONFIGURATION 3:......19

Default Configuration 3.1: TAR-EN1......19

Default Configuration 3.2: TAR-SGW1......20

IKEv2Interop.1.1: The Initial Exchanges......21

IKEv2Interop.1.2: Rekeying CHILD_SA......24

IKEv2Interop.1.3: Rekeying IKE_SA......28

IKEv2Interop.1.4: Cryptographic Algorithm Negotiation for IKE_SA......32

IKEv2Interop.1.5: Cryptographic Algorithm Negotiation for CHILD_SA......35

IKEv2Interop.1.6: Perfect Forward Secrecy......38

IKEv2Interop.1.7: Identification Type......40

IKEv2Interop.1.8: Multiple Proposals for IKE_SA......41

IKEv2Interop.1.9: Multiple Transforms for IKE_SA......45

IKEv2Interop.1.10: Multiple Proposals for CHILD_SA......49

IKEv2Interop.1.11: Multiple Transforms for CHILD_SA......53

IKEv2Interop.1.12: Requesting an Internal Address on a Remote Network......................57

IKEv2Interop.1.13: RSA Digital Signature..59

Appendix A..62

1. REQUIRED DATA 63

1.1. Test Data...64

1.2. Data file name syntax 67

1.3. Data Archive...70

1.4. Network Traffic Application 71

Requirements

To obtain the IPv6 Ready Logo Phase-2 for IKEv2, the target device must satisfy all of the following requirements.

Equipment Type

There are two possibilities for equipment types:

End-Node:

A node who can use IKEv2 (IPsec transport mode and tunnel mode) only for itself. Host and Router can be an End-Node

SGW (Security Gateway):

A node who can provide IKEv2 (IPsec tunnel mode) for nodes behind it. Router can be a SGW

Function List

Basic/Advanced Functionality table

This interoperability test scenario consists following BASIC/ADVANCED functions. The tests for ADVANCED functions may be omitted if the target device does not support the ADVANCED function.

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

Parameter		**BASIC**	**ADVANCED**
Exchange Type		Initial Exchanges (IKE_INIT, IKE_AUTH)	-
		CREATE_CHILD_SA	-
		INFORMATIONAL	-
IKE_SA	**Encryption Algorithm**	ENCR_3DES	ENCR_AES_CBC
	Pseudo-random Function	PRF_HMAC_SHA1	PRF_AES128_XCBC PRF_HMAC_SHA2_256
	Integrity Algorithm	AUTH_HMAC_SHA1_96	AUTH_AES_XCBC_96 AUTH_HAMC_SHA2_256_128
	Diffie-Hellman Group	2 (1024 MODP Group)	14 (2048 MODP Group) 24 (2048 MODP Group with 256-bit Prime Order Subgroup)
CHILD_SA	**Encryption Algorithm**	ENCR_3DES	ENCR_AES_CBC ENCR_AES_CTR ENCR_NULL
	Integrity Algorithm	AUTH_HMAC_SHA1_96	AUTH_AES_XCBC_96 NONE AUTH_HMAC_SHA2_256_128
	ESN	Disable	Enable
Authentication Method		PSK	RSA Digital Signature
Security Protocol		ESP	-
Encapsulation mode	**End-Node**	Transport	Tunnel
	SGW	Tunnel	-
Multiple Proposals		Receiving	Sending
Multiple Transforms		Receiving	Sending
Liveness Check		Support	-
Cookies		-	Support
Rekeying		Support	-
Traffic Selector Negotiation		Support	-

Requesting an Internal Address on a Remote Network	-	Support
PFS	-	Support
Closing SAs	Support	-
ID Type	ID_IPV6_ADDR	-
Creating Additional CHILD_SA	-	Support

Tests performed on End-Node/SGW

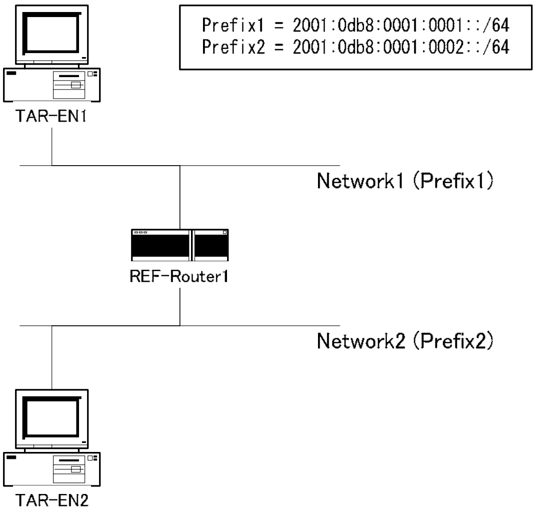
The tests under the End-Node/SGW column marked by a "(BASIC)" must be performed as specified below. If the End-Node/SGW supports the particular ADVANCED function, the corresponding tests under the End-Node/SGW column marked by a "(ADVANCED)" must be performed. If there is no "(BASIC)" or "(ADVANCED)" listed under the End-Node/SGW column, this test may be omitted.

	Part	End-Nodes	SGWs	Required ADVANCED function
IKEv2Interop.1.1	A	(BASIC)	-	
	B	(BASIC)	-	
	C	-	(BASIC)	
	D	-	(BASIC)	
	E	(ADVANCED)	-	End-Node Tunnel Mode
	F	(ADVANCED)	-	End-Node Tunnel Mode
IKEv2Interop.1.2	A	(BASIC)	-	
	B	(BASIC)	-	
	C	-	(BASIC)	
	D	-	(BASIC)	
IKEv2Interop.1.3	A	(BASIC)	-	
	B	(BASIC)	-	
	C	-	(BASIC)	
	D	-	(BASIC)	
AIKEv2Interop.1.4	A	(ADVANCED)	-	ENCR_AES_CBC for IKE_SA encryption algorithm
	~~B~~	(ADVANCED)	-	ENCR_AES_CTR for IKE_SA encryption algorithm
	C	(ADVANCED)	-	PRF_AES128_CBC for IKE_SA PRF
	D	(ADVANCED)	-	AUTH_AES_XCBC_96 for IKE_SA integrity algorithm
	E	(ADVANCED)	-	14 (2048 MODP Group) for IKE_SA DH Group
	F	(ADVANCED)	-	ENCR_AES_CBC for IKE_SA encryption algorithm
	~~G~~	(ADVANCED)	-	ENCR_AES_CTR for IKE_SA encryption algorithm
	H	(ADVANCED)	-	PRF_AES128_CBC for IKE_SA PRF
	I	(ADVANCED)	-	AUTH_AES_XCBC_96 for IKE_SA integrity algorithm
	J	(ADVANCED)	-	14 (2048 MODP Group) for IKE_SA DH Group
	K	-	(ADVANCED)	ENCR_AES_CBC for IKE_SA encryption algorithm
	~~L~~	-	(ADVANCED)	ENCR_AES_CTR for IKE_SA encryption algorithm
	M	-	(ADVANCED)	PRF_AES128_CBC for IKE_SA PRF
	N	-	(ADVANCED)	AUTH_AES_XCBC_96 for IKE_SA integrity algorithm
	O	-	(ADVANCED)	14 (2048 MODP Group) for IKE_SA DH Group
	P	-	(ADVANCED)	ENCR_AES_CBC for IKE_SA encryption algorithm
	~~Q~~	-	(ADVANCED)	ENCR_AES_CTR for IKE_SA encryption algorithm
	R	-	(ADVANCED)	PRF_AES128_CBC for IKE_SA PRF
	S	-	(ADVANCED)	AUTH_AES_XCBC_96 for IKE_SA integrity algorithm
	T	-	(ADVANCED)	14 (2048 MODP Group) for IKE_SA DH Group
	AA	(ADVANCED)	-	PRF_HMAC_SHA2_256 for IKE_SA PRF
	BB	(ADVANCED)	-	PRF_HMAC_SHA2_256 for IKE_SA PRF
	CC	(ADVANCED)	-	AUTH_HMAC_SHA2_256_128 for IKE_SA integrity algorithm
	DD	(ADVANCED)	-	AUTH_HMAC_SHA2_256_128 for IKE_SA integrity algorithm
	EE	(ADVANCED)	-	24 (2048 MODP Group with 256-bit Prime Order Subgroup) for IKE_SA DH Group
	FF	(ADVANCED)	-	24 (2048 MODP Group with 256-bit Prime Order Subgroup) for IKE_SA DH Group
	GG	-	(ADVANCED)	PRF_HMAC_SHA2_256 for IKE_SA PRF
	HH	-	(ADVANCED)	PRF_HMAC_SHA2_256 for IKE_SA PRF
	II	-	(ADVANCED)	AUTH_HMAC_SHA2_256_128 for IKE_SA integrity algorithm
	JJ	-	(ADVANCED)	AUTH_HMAC_SHA2_256_128 for IKE_SA integrity algorithm
	KK	-	(ADVANCED)	24 (2048 MODP Group with 256-bit Prime Order Subgroup) for IKE_SA DH Group
	LL	-	(ADVANCED)	24 (2048 MODP Group with 256-bit Prime Order Subgroup) for IKE_SA DH Group
IKEv2Interop.1.5	A	(ADVANCED)	-	ENCR_AES_CBC for CHILD_SA encryption algorithm
	B	(ADVANCED)	-	ENCR_AES_CTR for CHILD_SA encryption algorithm
	C	(ADVANCED)	-	ENCR_NULL for CHILD_SA encryption algorithm
	D	(ADVANCED)	-	AUTH_AES_XCBC_96 for CHILD_SA encryption algorithm
	E	(ADVANCED)	-	NONE for IKE_SA encryption algorithm
	F	(ADVANCED)	-	Enabling ESN
	G	(ADVANCED)	-	ENCR_AES_CBC for CHILD_SA encryption algorithm

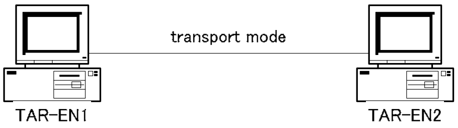
	H	(ADVANCED)	-	ENCR_AES_CTR for CHILD_SA encryption algorithm
	I	(ADVANCED)	-	ENCR_NULL for CHILD_SA encryption algorithm
	J	(ADVANCED)	-	AUTH_AES_XCBC_96 for CHILD_SA encryption algorithm
	K	(ADVANCED)	-	NONE for IKE_SA encryption algorithm
	L	(ADVANCED)	-	Enabling ESN
	M	-	(ADVANCED)	ENCR_AES_CBC for CHILD_SA encryption algorithm
	N	-	(ADVANCED)	ENCR_AES_CTR for CHILD_SA encryption algorithm
	O	-	(ADVANCED)	ENCR_NULL for CHILD_SA encryption algorithm
	P	-	(ADVANCED)	AUTH_AES_XCBC_96 for CHILD_SA encryption algorithm
	Q	-	(ADVANCED)	NONE for IKE_SA encryption algorithm
	R	-	(ADVANCED)	Enabling ESN
	S	-	(ADVANCED)	ENCR_AES_CBC for CHILD_SA encryption algorithm
	T	-	(ADVANCED)	ENCR_AES_CTR for CHILD_SA encryption algorithm
	U	-	(ADVANCED)	ENCR_NULL for CHILD_SA encryption algorithm
	V	-	(ADVANCED)	AUTH_AES_XCBC_96 for CHILD_SA encryption algorithm
	W	-	(ADVANCED)	NONE for IKE_SA encryption algorithm
	X	-	(ADVANCED)	Enabling ESN
	AA	(ADVANCED)	-	AUTH_HMAC_SHA2_256_128 for CHILD_SA integrity algorithm
	BB	(ADVANCED)	-	AUTH_HMAC_SHA2_256_128 for CHILD_SA integrity algorithm
	CC	-	(ADVANCED)	AUTH_HMAC_SHA2_256_128 for CHILD_SA integrity algorithm
	DD	-	(ADVANCED)	AUTH_HMAC_SHA2_256_128 for CHILD_SA integrity algorithm
IKEv2Interop.1.6	A	(ADVANCED)	-	Enabling PFS
	B	(ADVANCED)	-	Enabling PFS
	C	-	(ADVANCED)	Enabling PFS
	D	-	(ADVANCED)	Enabling PFS
~~IKEv2Interop.1.7~~				Removed at version 1.0.1
IKEv2Interop.1.8	A	(ADVANCED)	-	Transmitting Multiple Proposals for IKE_SA
	B	(BASIC)	-	
	C	-	(ADVANCED)	Transmitting Multiple Proposals for IKE_SA
	D	-	(BASIC)	
IKEv2Interop.1.9	A	(ADVANCED)	-	Transmitting Multiple Transforms for IKE_SA
	B	(ADVANCED)	-	Transmitting Multiple Transforms for IKE_SA
	C	(ADVANCED)	-	Transmitting Multiple Transforms for IKE_SA
	D	(ADVANCED)	-	Transmitting Multiple Transforms for IKE_SA
	E	(BASIC)	-	
	F	(BASIC)	-	
	G	(BASIC)	-	
	H	(BASIC)	-	
	I	-	(ADVANCED)	Transmitting Multiple Transforms for IKE_SA
	J	-	(ADVANCED)	Transmitting Multiple Transforms for IKE_SA
	K	-	(ADVANCED)	Transmitting Multiple Transforms for IKE_SA
	L	-	(ADVANCED)	Transmitting Multiple Transforms for IKE_SA
	M	-	(BASIC)	
	N	-	(BASIC)	
	O	-	(BASIC)	
	P	-	(BASIC)	
IKEv2Interop.1.10	A	(ADVANCED)	-	Transmitting Multiple Proposals for CHILD_SA
	B	(BASIC)	-	
	C	-	(ADVANCED)	Transmitting Multiple Proposals for CHILD_SA
	D	-	(BASIC)	
IKEv2Interop.1.11	A	(ADVANCED)	-	Transmitting Multiple Transforms for CHILD_SA
	B	(ADVANCED)	-	Transmitting Multiple Transforms for CHILD_SA
	C	(ADVANCED)	-	Transmitting Multiple Transforms for CHILD_SA
	D	(BASIC)	-	
	E	(BASIC)	-	
	F	(BASIC)	-	
	G	-	(ADVANCED)	Transmitting Multiple Transforms for CHILD_SA
	H	-	(ADVANCED)	Transmitting Multiple Transforms for CHILD_SA
	I	-	(ADVANCED)	Transmitting Multiple Transforms for CHILD_SA
	J	-	(BASIC)	
	K	-	(BASIC)	
	L	-	(BASIC)	
IKEv2Interop.1.12	A	(ADVANCED)	(ADVANCED)	Requesting/Replying an Internal Address on a Remote Network
IKEv2Interop.1.13	A	(ADVANCED)	-	RSA Digital Signature
	B	(ADVANCED)	-	RSA Digital Signature
	C	-	(ADVANCED)	RSA Digital Signature
	D	-	(ADVANCED)	RSA Digital Signature

Scenario 1: End-Node to End-Node Transport Mode

Default Network Topology 1:


Prefix1 = 2001:0db8:0001:0001::/64
Prefix2 = 2001:0db8:0001:0002::/64
TAR-EN1
Network1 (Prefix1)
REF-Router1
Network2 (Prefix2)
TAR-EN2

The transport mode is used in this topology.



The common network topology involves End-Node and Router devices on each link.

TAR-EN1:	Applicant Implementation	*1
TAR-EN2:	Vendor A/B End-Node	*1
REF-Router1:	Any Router	

*1) Must have an ability to use a ping6 application and print out results indicating the receipt of an ICMPv6 Echo Reply

Default Configuration 1:

Default Configuration 1.1: TAR-EN1

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	Key Value	Type	Data	
Local	TAR-EN1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-EN1	Disable
Remote	TAR-EN2	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-EN2	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR -EN1 is the initiator, above proposal must be included. Otherwise, TAR-EN1 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	Integrity	ESN
Inbound	ESP	Transport	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

*) When TAR-EN1 is the initiator, above proposal must be included. Otherwise, TAR-EN1 must select above proposal.

	Traffic Selector					
	Source			Destination		
	Address Range	Next Layer Protocol	Port Range	Address Range	Next Layer Protocol	Port Range
Inbound	TAR-EN2	ANY	ANY	TAR-EN1	ANY	ANY
Outbound	TAR-EN1	ANY	ANY	TAR-EN2	ANY	ANY

*) When TAR-EN1 is the initiator, TAR-EN1 must propose Traffic Selector covering above address range. Otherwie, TAR-EN1 must narrow Traffic Selector to above address range.

Default Configuration 1.2: TAR-EN2

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	**Key Value**	**Type**	**Data**	
Local	TAR-EN2	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-EN2	Disable
Remote	TAR-EN1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-EN1	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR-EN2 is the initiator, above proposal must be included. Otherwise, TAR-EN2 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	**Integrity**	**ESN**
Inbound	ESP	Transport	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

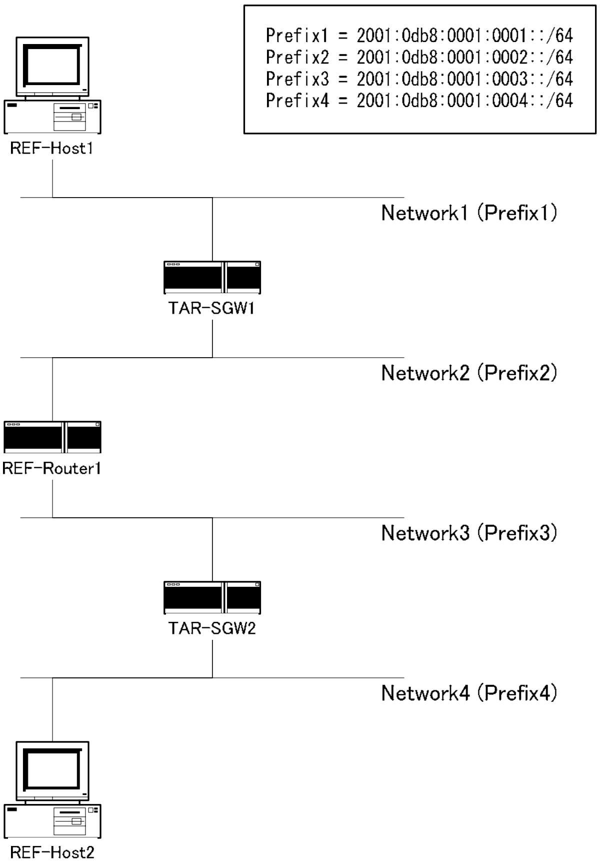
*) When TAR-EN2 is the initiator, above proposal must be included. Otherwise, TAR-EN2 must select above proposal.

	Traffic Selector					
	Source			**Destination**		
	Address Range	**Next Layer Protocol**	**Port Range**	**Address Range**	**Next Layer Protocol**	**Port Range**
Inbound	TAR-EN1	ANY	ANY	TAR-EN2	ANY	ANY
Outbound	TAR-EN2	ANY	ANY	TAR-EN1	ANY	ANY

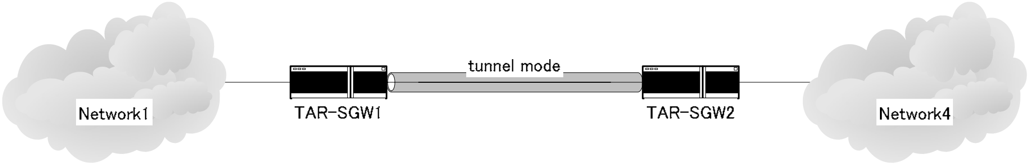
*) When TAR-EN2 is the initiator, TAR-EN2 must propose Traffic Selector covering above address range. Otherwie, TAR-EN2 must narrow Traffic Selector to above address range.

Scenario 2: SGW to SGW Tunnel Mode

Default Network Topology 2:


Prefix1 = 2001:0db8:0001:0001::/64
Prefix2 = 2001:0db8:0001:0002::/64
Prefix3 = 2001:0db8:0001:0003::/64
Prefix4 = 2001:0db8:0001:0004::/64
REF-Host1
Network1 (Prefix1)
TAR-SGW1
Network2 (Prefix2)
REF-Router1
Network3 (Prefix3)
TAR-SGW2
Network4 (Prefix4)
REF-Host2

The tunnel mode is used in this topology.



The common network topology involves SGW, Router and Host devices on each link.

TAR-SGW1:	Applicant Implementation	
TAR-SGW2:	Vendor C/D SGW	
REF-Router1:	Any Router	
REF-Host1:	Any Host	*1
REF-Host2:	Any Host	*1

*1) Must have an ability to use a ping6 application and print out results indicating the receipt of an ICMPv6 Echo Reply

Default Configuration 2:

Default Configuration 2.1: TAR-SGW1

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	Key Value	Type	Data	
Local	TAR-SGW1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-SGW1	Disable
Remote	TAR-SGW2	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-SGW2	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR-SGW1 is the initiator, above proposal must be included. Otherwise, TAR-SGW1 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	Integrity	ESN
Inbound	ESP	Tunnel	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

*) When TAR-SGW1 is the initiator, above proposal must be included. Otherwise, TAR-SGW1 must select above proposal.

	Traffic Selector					
	Source			Destination		
	Address Range	Next Layer Protocol	Port Range	Address Range	Next Layer Protocol	Port Range
Inbound	Network4	ANY	ANY	Network1	ANY	ANY
Outbound	Network1	ANY	ANY	Network4	ANY	ANY

*) When TAR-SGW1 is the initiator, TAR-SGW1 must propose Traffic Selector covering above address range. Otherwie, TAR-SGW1 must narrow Traffic Selector to above address range.

Default Configuration 2.2: TAR-SGW2

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	Key Value	Type	Data	
Local	TAR-SGW2	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-SGW2	Disable
Remote	TAR-SGW1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-SGW1	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR-SGW2 is the initiator, above proposal must be included. Otherwise, TAR-SGW2 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	Integrity	ESN
Inbound	ESP	Tunnel	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

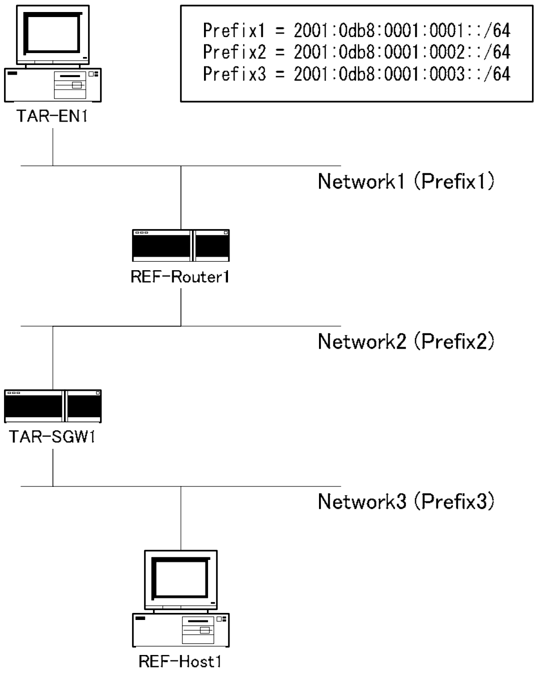
*) When TAR-SGW2 is the initiator, above proposal must be included. Otherwise, TAR-SGW2 must select above proposal.

	Traffic Selector					
	Source			Destination		
	Address Range	Next Layer Protocol	Port Range	Address Range	Next Layer Protocol	Port Range
Inbound	Network1	ANY	ANY	Network4	ANY	ANY
Outbound	Network4	ANY	ANY	Network1	ANY	ANY

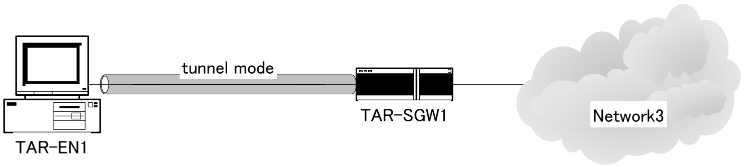
*) When TAR-SGW2 is the initiator, TAR-SGW2 must propose Traffic Selector covering above address range. Otherwie, TAR-SGW2 must narrow Traffic Selector to above address range.

Scenario 3: End-Node to SGW/SGW to End-Node Tunnel Mode

Default Network Topology 3:


TAR-EN1
Prefix1 = 2001:0db8:0001:0001::/64
Prefix2 = 2001:0db8:0001:0002::/64
Prefix3 = 2001:0db8:0001:0003::/64
Network1 (Prefix1)
REF-Router1
Network2 (Prefix2)
TAR-SGW1
Network3 (Prefix3)
REF-Host1

The tunnel mode is used in this topology.



The common network topology involves End-Node, SGW, Router and Host devices on each link.

	if the Applicant Implementation is an End-Node	**if the Applicant Implementation is a SGW**	
TAR-EN1:	Applicant Implementation	Vendor A/B End-Node	*1
TAR-SGW1:	Vendor C/D SGW	Applicant Implementation	
REF-Router1:	Any Router		
REF-Host1:	Any Host		*1

*1) Must have an ability to use a ping6 application and print out results indicating the receipt of an ICMPv6 Echo Reply

Default Configuration 3:

Default Configuration 3.1: TAR-EN1

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	Key Value	Type	Data	
Local	TAR-EN1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-EN1	Disable
Remote	TAR-SGW1	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-SGW1	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR-EN1 is the initiator, above proposal must be included. Otherwise, TAR-EN1 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	Integrity	ESN
Inbound	ESP	Tunnel	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

*) When TAR-EN1 is the initiator, above proposal must be included. Otherwise, TAR-EN1 must select above proposal.

	Traffic Selector					
	Source			Destination		
	Address Range	Next Layer Protocol	Port Range	Address Range	Next Layer Protocol	Port Range
Inbound	Network3	ANY	ANY	TAR-EN1	ANY	ANY
Outbound	TAR-EN1	ANY	ANY	Network3	ANY	ANY

*) When TAR-EN1 is the initiator, TAR-EN1 must propose Traffic Selector covering above address range. Otherwie, TAR-EN1 must narrow Traffic Selector to above address range.

Default Configuration 3.2: TAR-SGW1

IKE Peer

	Address	Port	Authentication		ID		PFS
			Method	Key Value	Type	Data	
Local	TAR-SGW1	500	PSK	IKETEST456!	ID_IPV6_ADDR	TAR-SGW1	Disable
Remote	TAR-EN1	500	PSK	IKETEST123!	ID_IPV6_ADDR	TAR-EN1	

IKE_SA

Cryptographic Algorithms			
Encryption	**PRF**	**Integrity**	**Diffie-Hellman**
ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)

*) When TAR-SGW1 is the initiator, above proposal must be included. Otherwise, TAR-SGW1 must select above proposal.

CHILD_SA

	Security Protocol	Mode	Cryptographic Algorithms		
			Encryption	**Integrity**	**ESN**
Inbound	ESP	Tunnel	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Outbound					

*) When TAR-SGW1 is the initiator, above proposal must be included. Otherwise, TAR-SGW1 must select above proposal.

	Traffic Selector					
	Source			**Destination**		
	Address Range	**Next Layer Protocol**	**Port Range**	**Address Range**	**Next Layer Protocol**	**Port Range**
Inbound	TAR-EN1	ANY	ANY	Network3	ANY	ANY
Outbound	Network3	ANY	ANY	TAR-EN1	ANY	ANY

*) When TAR-SGW1 is the initiator, TAR-SGW1 must propose Traffic Selector covering above address range. Otherwie, TAR-SGW1 must narrow Traffic Selector to above address range.

IKEv2Interop.1.1: The Initial Exchanges

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions.

References:

- [IKEv2] – Section 1.2

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2
  - *Part E - F*
    Default Network Topology 3

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A - B*
    Default Configuration 1
  - *Part C - D*
    Default Configuration 2
  - *Part E - F*
    Default Configuration 3

Procedure:

Part A: End-Node to End-Node #1 (BASIC)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (BASIC)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part E: End-Node to SGW (ADVANCED)

13. Initialize TAR-EN1 and TAR-SGW1 making sure they have cleared their Security Associations.
14. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of REF-Host1.
15. Observe the packets transmitted on Network1, Network2 and Network3.

Part F: SGW to End-Node (ADVANCED)

16. Initialize TAR-EN1 and TAR-SGW1 making sure they have cleared their Security Associations.
17. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of TAR-EN1.
18. Observe the packets transmitted on Network1, Network2 and Network3.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Part E

Step 15:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network1 and Network2, and they are decrypted on Network3. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Part F

Step 18:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network1 and Network2, and they are decrypted on Network3. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Possible Problems:

- None.

IKEv2Interop.1.2: Rekeying CHILD_SA

Purpose:

To verify that a successful Rekeying can be achieved in two directions for CHILD_SA.

References:

- [IKEv2] – Section 2.8

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A*
    - TAR-EN1
      In addition to the default configuration 1.1, configure CHILD_SA lifetime to be expired within short period (for example around 30 seconds) regardless of SA life type.
    - TAR-EN2
      In addition to the default configuration 1.2, configure enough long CHILD_SA lifetime (for example 300 seconds) regardless of SA life type not to be expired before TAR-EN1's lifetime expires.
  - *Part B*
    - TAR-EN1
      In addition to the default configuration 1.1, configure enough long CHILD_SA lifetime (for example 300 seconds) regardless of SA life type not to be expired before TAR-EN2's lifetime expires.
    - TAR-EN2
      In addition to the default configuration 1.2, configure CHILD_SA lifetime to be expired within short period (for example around 30 seconds) regardless of SA life type.
  - *Part C*
    - TAR-SGW1
      In addition to the default configuration 2.1, configure CHILD_SA lifetime to be expired within short period (for example around 30 seconds) regardless of SA life type.
    - TAR-SGW2

In addition to the default configuration 2.2, configure enough long CHILD_SA lifetime (for example 300 seconds) regardless of SA life type not to be expired before TAR-SGW1's lifetime expires.

- *Part D*
  - ✧ TAR-SGW1

    In addition to the default configuration 2.1, configure enough long CHILD_SA lifetime (for example 300 seconds) regardless of SA life type not to be expired before TAR-SGW2's lifetime expires.
  - ✧ TAR-SGW2

    In addition to the default configuration 2.2, configure CHILD_SA lifetime to be expired within short period (for example around 30 seconds) regardless of SA life type.

Procedure:

Part A: End-Node to End-Node #1 (BASIC)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2 for enough long period (for example 60 seconds if TAR-EN1's CHILD_SA lifetime is 30 seconds) until TAR-EN1's CHILD_SA lifetime expires.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1 for enough long period (for example 60 seconds if TAR-EN2's CHILD_SA lifetime is 30 seconds) until TAR-EN2's CHILD_SA lifetime expires.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (BASIC)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2 for enouth long period (for example 60 seconds if TAR-SGW1's CHILD_SA lifetime is 30 seconds) until TAR-SGW1's CHILD_SA lifetime expires.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1 for enouth long period (for example 60 seconds if TAR-SGW2's CHILD_SA lifetime is 30 seconds) until TAR-SGW2's CHILD_SA lifetime expires.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Before TAR-EN1's CHILD_SA lifetime expires (for example less than 30 seconds passed if TAR-EN1's CHILD_SA lifetime is 30 seconds), TAR-EN1 initiates the rekeying for CHILD_SA and CHILD_SAs are updated. Then each SPI in ESP is updated. The ping6 application result on TAR-EN1 keeps indicating the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Before TAR-EN2's CHILD_SA lifetime expires (for example less than 30 seconds passed if TAR-EN2's CHILD_SA lifetime is 30 seconds), TAR-EN2 initiates the rekeying for CHILD_SA and CHILD_SAs are updated. Then each SPI in ESP is updated. Then each SPI in ESP is updated. The ping6 application result on TAR-EN2 keeps indicating the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Before TAR-SGW1's CHILD_SA lifetime expires (for example less than 30 seconds passed if TAR-SGW1's CHILD_SA lifetime is 30 seconds), TAR-SGW1 initiates the rekeying for CHILD_SA and CHILD_SAs are updated. Then each SPI in ESP is updated. The ping6 application result on REF-Host1 keeps indicating the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Before TAR-SGW2's CHILD_SA lifetime expires (for example less than 30 seconds passed if TAR-SGW2's CHILD_SA lifetime is 30 seconds), TAR-SGW2 initiates the rekeying for CHILD_SA and CHILD_SAs are updated. Then each SPI in ESP is updated. The ping6 application result on REF-Host2 keeps indicating the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- Since

IKEv2Interop.1.3: Rekeying IKE_SA

Purpose:

To verify that a successful Rekeying can be achieved in two directions for IKE_SA.

References:

- [IKEv2] – Section 2.18

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A*
    - TAR-EN1
      In addition to the default configuration 1.1, configure IKE_SA lifetime and CHILD_SA lifetime to be expired within short period (for example around 40 seconds for IKE_SA lifetime and around 30 seconds for CHILD_SA lifetime) regardless of SA life type.
    - TAR-EN2
      In addition to the default configuration 1.2, configure enough long IKE_SA lifetime and CHILD_SA lifetime (for example 400 seconds for IKE_SA lifetime and 300 seconds for CHILD_SA lifetime) regardless of SA life type not to be expired before TAR-EN1's lifetime expires.
  - *Part B*
    - TAR-EN1
      In addition to the default configuration 1.1, configure enough long IKE_SA lifetime and CHILD_SA lifetime (for example 400 seconds for IKE_SA lifetime and 300 seconds for CHILD_SA lifetime) regardless of SA life type not to be expired before TAR-EN2's lifetime expires.
    - TAR-EN2
      In addition to the default configuration 1.2, configure IKE_SA lifetime and CHILD_SA lifetime to be expired within short period (for example around 40 seconds for IKE_SA lifetime and around 30 seconds for CHILD_SA lifetime) regardless of SA life type.
  - *Part C*
    - TAR-SGW1

In addition to the default configuration 2.1, configure IKE_SA lifetime and CHILD_SA lifetime to be expired within short period (for example around 40 seconds for IKE_SA lifetime and around 30 seconds for CHILD_SA lifetime) regardless of SA life type.

- ✧ TAR-SGW2

  In addition to the default configuration 2.2, configure enough long IKE_SA lifetime and CHILD_SA lifetime (for example 400 seconds for IKE_SA lifetime and 300 seconds for CHILD_SA lifetime) regardless of SA life type not to be expired before TAR-SGW1's lifetime expires.

- ➢ *Part D*
  - ✧ TAR-SGW1

    In addition to the default configuration 2.1, configure enough long IKE_SA lifetime and CHILD_SA lifetime (for example 400 seconds for IKE_SA lifetime and 300 seconds for CHILD_SA lifetime) regardless of SA life type not to be expired before TAR-SGW2's lifetime expires.
  - ✧ TAR-SGW2

    In addition to the default configuration 2.2, configure IKE_SA lifetime and CHILD_SA lifetime to be expired within short period (for example around 40 seconds for IKE_SA lifetime and around 30 seconds for CHILD_SA lifetime) regardless of SA life type.

Procedure:

Part A: End-Node to End-Node #1 (BASIC)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2 for enough long period (for example 80 seconds if TAR-EN1's IKE_SA lifetime is 40 seconds) until TAR-EN1's IKE_SA lifetime expires.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1 for enough long period (for example 80 seconds if TAR-EN2's IKE_SA lifetime is 40 seconds) until TAR-EN2's IKE_SA lifetime expires.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (BASIC)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2 for enough long period (for example 80 seconds if TAR-SGW1's IKE_SA lifetime is 40 seconds) until TAR-SGW1's IKE_SA lifetime expires.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit continuous ICMPv6 Echo Requests from REF-Host2

to the Global unicast address of REF-Host1 for enough long period (for example 80 seconds if TAR-SGW2's IKE_SA lifetime is 40 seconds) until TAR-SGW2's IKE_SA lifetime expires.

12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Before TAR-EN1's IKE_SA lifetime expires (for example less than 40 seconds passed if TAR-EN1's IKE_SA lifetime is 40 seconds), TAR-EN1 initiates the rekeying for IKE_SA and IKE_SAs are updated independently of the rekeying for CHILD_SA. Then both SPIs in IKE header are updated. The ping6 application result on TAR-EN1 keeps indicating the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Before TAR-EN2's IKE_SA lifetime expires (for example less than 40 seconds passed if TAR-EN2's IKE_SA lifetime is 40 seconds), TAR-EN2 initiates the rekeying for IKE_SA and IKE_SAs are updated independently of the rekeying for CHILD_SA. Then both SPIs in IKE header are updated. The ping6 application result on TAR-EN2 keeps indicating the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Before TAR-SGW1's IKE_SA lifetime expires (for example less than 40 seconds passed if TAR-SGW1's IKE_SA lifetime is 40 seconds), TAR-SGW1 initiates the rekeying for IKE_SA and IKE_SAs are updated independently of the rekeying for CHILD_SA. Then both SPIs in IKE header are updated. The ping6 application result on REF-Host1 keeps indicating the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Before TAR-SGW2's IKE_SA lifetime expires (for example less than 40 seconds passed if TAR-SGW2's IKE_SA lifetime is 40 seconds), TAR-SGW2 initiates the rekeying for IKE_SA and IKE_SAs are updated independently of the rekeying for CHILD_SA. Then both SPIs in IKE header are updated. The ping6 application result on REF-Host2 keeps indicating the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.4: Cryptographic Algorithm Negotiation for IKE_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions with various combination of cryptographic algorithms for IKE_SA

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - ➢ *Part A - J*
    Default Network Topology 1
  - ➢ *Part K - T*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - ➢ *Part A - J, AA - FF*
    Default Configuration 1 with configuring IKE_SA cryptographic algorithms as describing below.

	Encryption	PRF	Integrity	Diffie-Hellman
Part A, F	ENCR_AES_CBC	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part B, G	REMOVED	REMOVED	REMOVED	REMOVED
Part C, H	ENCR_3DES	PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part D, I	ENCR_3DES	PRF_HMAC_SHA1	AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part E, J	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	14 (2048 MODP Group)
Part AA, BB	ENCR_3DES	PRF_HMAC_SHA2_256	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part CC, DD	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA2_256_128	2 (1024 MODP Group)
Part EE, FF	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	24 (2048 MODP Group with 256-bit Prime Order Subgroup)

  - ➢ *Part K - T, GG - LL*
    Default Configuration 2 with configuring IKE_SA cryptographic algorithms as describing below.

	Encryption	PRF	Integrity	Diffie-Hellman
Part K, P	ENCR_AES_CBC	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part L, Q	ENCR_AES_CTR	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part M, R	ENCR_3DES	PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part N, S	ENCR_3DES	PRF_HMAC_SHA1	AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part O, T	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	14 (2048 MODP Group)
Part GG, HH	ENCR_3DES	PRF_HMAC_SHA2_256	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part II, JJ	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA2_256_128	2 (1024 MODP Group)
Part KK, LL	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	24 (2048 MODP Group with 256-bit Prime Order Subgroup)

Procedure:

Part A - E, AA, CC, EE: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part F - J, BB, DD, FF: End-Node to End-Node #2 (ADVANCED)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part K - O, GG, II, KK: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part P - T, HH, JJ, LL: SGW to SGW #2 (ADVANCED)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A - E, AA, CC, EE

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part F - J, BB, DD, FF

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part K - O, GG, II, KK

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are

decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part P - T, HH, JJ, LL

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.5: Cryptographic Algorithm Negotiation for CHILD_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions with various combination of cryptographic algorithms for CHILD_SA.

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - L*
    Default Network Topology 1
  - *Part M - X*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A - L*
    Default Configuration 1 with configuring CHILD_SA cryptographic algorithms as describing below.

	Encryption	**Integrity**	**ESN**
Part A, G	ENCR_AES_CBC	AUTH_HMAC_SHA1_96	Disable
Part B, H	ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable
Part C, I	ENCR_NULL	AUTH_HMAC_SHA1_96	Disable
Part D, J	ENCR_3DES	AUTH_AES_XCBC_96	Disable
Part E, K	ENCR_3DES	NONE	Disable
Part F, L	ENCR_3DES	AUTH_HMAC_SHA1_96	Enable
Part AA, BB	ENCR_3DES	AUTH_HMAC_SHA2_256_128	Disable

  - *Part M - X*
    Default Configuration 2 with configuring CHILD_SA cryptographic algorithms as describing below.

	Encryption	**Integrity**	**ESN**
Part M, S	ENCR_AES_CBC	AUTH_HMAC_SHA1_96	Disable
Part N, T	ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable
Part O, U	ENCR_NULL	AUTH_HMAC_SHA1_96	Disable
Part P, V	ENCR_3DES	AUTH_AES_XCBC_96	Disable
Part Q, W	ENCR_3DES	NONE	Disable
Part R, X	ENCR_3DES	AUTH_HMAC_SHA1_96	Enable
Part CC, DD	ENCR_3DES	AUTH_HMAC_SHA2_256_128	Disable

Procedure:

Part A - F, AA: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part G - L, BB: End-Node to End-Node #2 (ADVANCED)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part M - R, CC: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part S - X, DD: SGW to SGW #2 (ADVANCED)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A - F, AA

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part G - L, BB

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part M - R, CC

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part S - X, DD

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.6: Perfect Forward Secrecy

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions using PFS.

References:

- [IKEv2] – Section 2.12

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A - B*
    Default Configuration 1 with enabling PFS
  - *Part C - D*
    Default Configuration 2 with enabling PFS

Procedure:

Part A: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (ADVANCED)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.

9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (ADVANCED)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.7: Identification Type

Removed at version 1.0.1.

IKEv2Interop.1.8: Multiple Proposals for IKE_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions by initiating multiple proposals for IKE_SA.

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below.
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below.
  - *Part A*
    - TAR-EN1
      Default Configuration 1.1 with configuring IKE_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

Proposal	Encryption	PRF	Integrity	Diffie-Hellman
Proposal #1	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Proposal #2	ENCR_3DES or ENCR_AES_CBC or ENCR_AES_CTR	PRF_HMAC_SHA1 or PRF_AES128_CBC	AUTH_HMAC_SHA1_96 or AUTH_AES_XCBC_96	2 (1024 MODP Group) or 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

    - TAR-EN2
      Default Configuration 1.2

  - *Part B*
    - TAR-EN1
      Default Configuration 1.1
    - TAR-EN2
      Default Configuration 1.2 with configuring IKE_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

Proposal	Encryption	PRF	Integrity	Diffie-Hellman
Proposal #1	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Proposal #2	ENCR_3DES or ENCR_AES_CBC or ENCR_AES_CTR	PRF_HMAC_SHA1 or PRF_AES128_CBC	AUTH_HMAC_SHA1_96 or AUTH_AES_XCBC_96	2 (1024 MODP Group) or 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

- *Part C*
  - TAR-SGW1

    Default Configuration 2.1 with configuring IKE_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

Proposal	Encryption	PRF	Integrity	Diffie-Hellman
Proposal #1	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Proposal #2	ENCR_3DES or ENCR_AES_CBC or ENCR_AES_CTR	PRF_HMAC_SHA1 or PRF_AES128_CBC	AUTH_HMAC_SHA1_96 or AUTH_AES_XCBC_96	2 (1024 MODP Group) or 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

  - TAR-SGW2

    Default Configuration 2.2

- *Part D*
  - TAR-SGW1

    Default Configuration 2.1
  - TAR-SGW2

    Default Configuration 2.2 with configuring IKE_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

Proposal	Encryption	PRF	Integrity	Diffie-Hellman
Proposal #1	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Proposal #2	ENCR_3DES or ENCR_AES_CBC or ENCR_AES_CTR	PRF_HMAC_SHA1 or PRF_AES128_CBC	AUTH_HMAC_SHA1_96 or AUTH_AES_XCBC_96	2 (1024 MODP Group) or 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

Procedure:

Part A: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security

Associations.

5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.9: Multiple Transforms for IKE_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions by initiating multiple transforms for IKE_SA.

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below
  - ➢ *Part A - H*
    Default Network Topology 1
  - ➢ *Part I - P*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below
  - ➢ *Part A - D*
    - ✧ TAR-EN1
      Default Configuration 1.1 with configuring IKE_SA cryptographic algorithms as describing below

	Encryption	PRF	Integrity	Diffie-Hellman
Part A	ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part B	ENCR_3DES	PRF_HMAC_SHA1 PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part C	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part D	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group), 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

    - ✧ TAR-EN2
      Default Configuration 1.2

  - ➢ *Part E - H*
    - ✧ TAR-EN1
      Default Configuration 1.1
    - ✧ TAR-EN2
      Default Configuration 1.2 with configuring IKE_SA cryptographic

algorithms as describing below

	Encryption	PRF	Integrity	Diffie-Hellman
Part E	ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part F	ENCR_3DES	PRF_HMAC_SHA1 PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part G	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part H	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group), 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

➢ *Part I - L*

✧ TAR-SGW1

Default Configuration 2.1 with configuring IKE_SA cryptographic algorithms as describing below

	Encryption	PRF	Integrity	Diffie-Hellman
Part I	ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part J	ENCR_3DES	PRF_HMAC_SHA1 PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part K	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part L	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group), 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

✧ TAR-SGW2

Default Configuration 2.2

➢ *Part M - P*

✧ TAR-SGW1

Default Configuration 2.1

✧ TAR-SGW2

Default Configuration 2.2 with configuring IKE_SA cryptographic algorithms as describing below

	Encryption	PRF	Integrity	Diffie-Hellman
Part M	ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part N	ENCR_3DES	PRF_HMAC_SHA1 PRF_AES128_CBC	AUTH_HMAC_SHA1_96	2 (1024 MODP Group)
Part O	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	2 (1024 MODP Group)
Part P	ENCR_3DES	PRF_HMAC_SHA1	AUTH_HMAC_SHA1_96	2 (1024 MODP Group), 14 (2048 MODP Group) or 24 (2048 MODP Group with 256-bit Prime Order Subgroup)

Procedure:

Part A - D: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part E - H: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part I - L: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part M - P: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A - D

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part E - H

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part I - L

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are

decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part M - P

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.10: Multiple Proposals for CHILD_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions by initiating multiple proposals for CHILD_SA

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below
  - *Part A - B*
    Default Network Topology 1
  - *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below
  - *Part A*
    - TAR-EN1
      Default Configuration 1.1 with configuring CHILD_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

Proposal	Encryption	Integrity	ESN
Proposal #1	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Proposal #2	ENCR_3DES or ENCR_NULL or ENCR_AES_CBC or ENCR_AES_CTR	AUTH_HMAC_SHA1_96 or NONE or AUTH_AES_XCBC_96	Disable or Enable

    - TAR-EN2
      Default Configuration 1.2

  - *Part B*
    - TAR-EN1
      Default Configuration 1.1

    - TAR-EN2
      Default Configuration 1.2 with configuring CHILD_SA cryptographic algorithms as describing below. Proposal #2 should be different transforms

from Proposal #1 as much as possible. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

	Encryption	Integrity	ESN
Proposal #1	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Proposal #2	ENCR_3DES or ENCR_NULL or ENCR_AES_CBC or ENCR_AES_CTR	AUTH_HMAC_SHA1_96 or NONE or AUTH_AES_XCBC_96	Disable or Enable

- *Part C*
  - TAR-SGW1

    Default Configuration 2.1 with configuring CHILD_SA cryptographic algorithms as describing below. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

	Encryption	Integrity	ESN
Proposal #1	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Proposal #2	ENCR_3DES or ENCR_NULL or ENCR_AES_CBC or ENCR_AES_CTR	AUTH_HMAC_SHA1_96 or NONE or AUTH_AES_XCBC_96	Disable or Enable

  - TAR-SGW2

    Default Configuration 2.2

- *Part D*
  - TAR-SGW1

    Default Configuration 2.1

  - TAR-SGW2

    Default Configuration 2.2 with configuring CHILD_SA cryptographic algorithms as describing below. At least one of transforms in proposal #2 must be different from corresponding transform in Proposal #1.

	Encryption	Integrity	ESN
Proposal #1	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable
Proposal #2	ENCR_3DES or ENCR_NULL or ENCR_AES_CBC or ENCR_AES_CTR	AUTH_HMAC_SHA1_96 or NONE or AUTH_AES_XCBC_96	Disable or Enable

Procedure:

Part A: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are

decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.11: Multiple Transforms for CHILD_SA

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions by initiating multiple transforms for CHILD_SA.

References:

- [IKEv2] – Section 2.7

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below
  - ➢ *Part A - F*
    Default Network Topology 1
  - ➢ *Part J - L*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below
  - ➢ *Part A - C*
    - ✧ TAR-EN1
      Default Configuration 1.1 with configuring CHILD_SA cryptographic algorithms as describing below

	Encryption	Integrity	ESN
Part A	ENCR_3DES ENCR_NULL or ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable
Part B	ENCR_3DES	AUTH_HMAC_SHA1_96 NONE or AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	Disable
Part C	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable Enable

    - ✧ TAR-EN2
      Default Configuration 1.2

  - ➢ *Part D - F*
    - ✧ TAR-EN1
      Default Configuration 1.1

- TAR-EN2

  Default Configuration 1.2 with configuring CHILD_SA cryptographic algorithms as describing below

	Encryption	Integrity	ESN
Part D	ENCR_3DES ENCR_NULL or ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable
Part E	ENCR_3DES	AUTH_HMAC_SHA1_96 NONE or AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	Disable
Part F	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable Enable

- *Part G - I*
  - TAR-SGW1

    Default Configuration 2.1 with configuring CHILD_SA cryptographic algorithms as describing below

	Encryption	Integrity	ESN
Part G	ENCR_3DES ENCR_NULL or ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable
Part H	ENCR_3DES	AUTH_HMAC_SHA1_96 NONE or AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	Disable
Part I	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable Enable

  - TAR-SGW2

    Default Configuration 2.2

- *Part J - L*
  - TAR-SGW1

    Default Configuration 2.1

  - TAR-SGW2

    Default Configuration 2.2 with configuring CHILD_SA cryptographic algorithms as describing below

	Encryption	Integrity	ESN
Part J	ENCR_3DES ENCR_NULL or ENCR_3DES ENCR_AES_CBC or ENCR_3DES ENCR_AES_CTR	AUTH_HMAC_SHA1_96	Disable

Part K	ENCR_3DES	AUTH_HMAC_SHA1_96 NONE or AUTH_HMAC_SHA1_96 AUTH_AES_XCBC_96	Disable
Part L	ENCR_3DES	AUTH_HMAC_SHA1_96	Disable Enable

Procedure:

Part A - C: End-Node to End-Node #1 (ADVANCED)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part D - F: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part G - I: SGW to SGW #1 (ADVANCED)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part J - L: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A - C

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part D - F

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part G - I

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part J - L

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.12: Requesting an Internal Address on a Remote Network

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions by using Configuration payloads.

References:

- [IKEv2] – Section 2.19

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures in Default Network Topology 3

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below
  - *Part A*
    - ✧ TAR-EN1
      Default Configuration 3 with the configuration to request INTERNAL_IP6_ADDRESS by CFG_REQUEST.
      Traffic Selector must cover the following.

	Source			**Destination**		
	Address Range	**Next Layer Protocol**	**Port Range**	**Address Range**	**Next Layer Protocol**	**Port Range**
Inbound	Network3	ANY	ANY	TAR-EN1 (internal address given by TAR-SGW1)	ANY	ANY
Outbound	TAR-EN1 (internal address given by TAR-SGW1)	ANY	ANY	Network3	ANY	ANY

- ✧ TAR-SGW1
  Default Configuration 3 with the configuration to accept CFG_REQUEST and to distribute the appropriate address (for example 2001:db8:1:4::1/64) by CFG_REPLY.
  Traffic Selector must cover the following.

	Source			**Destination**		
	Address Range	**Next Layer Protocol**	**Port Range**	**Address Range**	**Next Layer Protocol**	**Port Range**
Inbound	TAR-EN1 (internal address given by TAR-SGW1)	ANY	ANY	Network3	ANY	ANY
Outbound	Network3	ANY	ANY	TAR-EN1 (internal address given by TAR-SGW1)	ANY	ANY

Procedure:

Part A: End-Node to SGW (ADVANCED)

1. Initialize TAR-EN1 and TAR-SGW1 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of REF-Host1.
3. Observe the packets transmitted on Network1, Network2 and Network3.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network1 and Network2, and they are decrypted on Network3. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

IKEv2Interop.1.13: RSA Digital Signature

Purpose:

To verify that a successful Initial Exchange can be achieved in two directions using RSA Digital Signature as the authentication method.

References:

- [IKEv2] – Section 2.15

Resource Requirements:

- Monitor to capture packets
- Ping6 implementations

Test Setup:

- Network Topology
  For each Part, connect End-Nodes, SGWs, Routers and Hosts as per the figures below
  - ➢ *Part A - B*
    Default Network Topology 1
  - ➢ *Part C - D*
    Default Network Topology 2

- Configuration
  For each Part, configure End-Nodes and SGWs as per the configurations below
  - ➢ *Part A – B*
    - ✧ TAR-EN1
      Default Configuration 1.1 with configuring IKE peer as describing below

	Authentication	
	Method	**Key Value**
Local	RSA digital signature	-
Remote	RSA digital signature	-

    - ✧ TAR-EN2
      Default Configuration 1.2 with configuring IKE peer as describing below

	Authentication	
	Method	**Key Value**
Local	RSA digital signature	-
Remote	RSA digital signature	-

  - ➢ *Part C – D*
    - ✧ TAR-SGW1
      Default Configuration 2.1 with configuring IKE peer as describing below

	Authentication	
	Method	**Key Value**
Local	RSA digital signature	-
Remote	RSA digital signature	-

    - ✧ TAR-SGW2
      Default Configuration 2.2 with configuring IKE peer as describing below

	Authentication	
	Method	Key Value
Local	RSA digital signature	-
Remote	RSA digital signature	-

For every case, RSA digital signature public keys can be exchanged between peers previously or can be installed into local or public CA.

Procedure:

Part A: End-Node to End-Node #1 (BASIC)

1. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
2. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN1 to the Global unicast address of TAR-EN2.
3. Observe the packets transmitted on Network1 and Network2.

Part B: End-Node to End-Node #2 (BASIC)

4. Initialize TAR-EN1 and TAR-EN2 making sure they have cleared their Security Associations.
5. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from TAR-EN2 to the Global unicast address of TAR-EN1.
6. Observe the packets transmitted on Network1 and Network2.

Part C: SGW to SGW #1 (BASIC)

7. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
8. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host1 to the Global unicast address of REF-Host2.
9. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Part D: SGW to SGW #2 (BASIC)

10. Initialize TAR-SGW1 and TAR-SGW2 making sure they have cleared their Security Associations.
11. Initiate IKEv2 exchange and transmit ICMPv6 Echo Requests from REF-Host2 to the Global unicast address of REF-Host1.
12. Observe the packets transmitted on Network1, Network2, Network3 and Network4.

Observable Results:

Part A

Step 3:

TAR-EN1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6 Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN1 indicates the receipt of ICMPv6 Echo Reply from TAR-EN2.

Part B

Step 6:

TAR-EN2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The ICMPv6 Echo Requests and ICMPv6

Echo Replies observed on Network1 and Network2 are encrypted by ESP. The ping6 application result on TAR-EN2 indicates the receipt of ICMPv6 Echo Reply from TAR-EN1.

Part C

Step 9:

TAR-SGW1 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host1 indicates the receipt of ICMPv6 Echo Reply from REF-Host2.

Part D

Step 12:

TAR-SGW2 initiates IKEv2 negotiation and SAs are established. ICMPv6 Echo Requests and ICMPv6 Echo Replies are passed on SAs. The observed ICMPv6 Echo Requests and ICMPv6 Echo Replies are encrypted by ESP on Network2 and Network3, and they are decrypted on Network1 and Network4. The ping6 application result on REF-Host2 indicates the receipt of ICMPv6 Echo Reply from REF-Host1.

Possible Problems:

- None.

Appendix A

1. Required Data

To obtain the IPv6 Ready Logo Phase-2 IKEv2, you need to send application with the test results attached.

The test results must include both Protocol Operations and Interoperability.
In this document, the **"Interoperability test"** result documentation is described.

There are currently two viable alternatives to obtain an interoperability results.

- Lab Test: Test results observed at a lab that is recognized by the IPv6 Ready Logo Committee.
- Self Test: Test results observed by the applicant company in their laboratory.

1.1. Test Data

As "IPv6 Ready Logo Phase-2 IKEv2" the following interoperability test result data are required.

Topology Map (Required)

Network topology figures or address list for each topology, with IPv6 addresses and MAC address of each attached interfaces, are required. Fig. 1 and Fig. 2 are examples of topology figure. Fig. 3 is an example of address list.

All IP addresses which are used during the test must be declared.

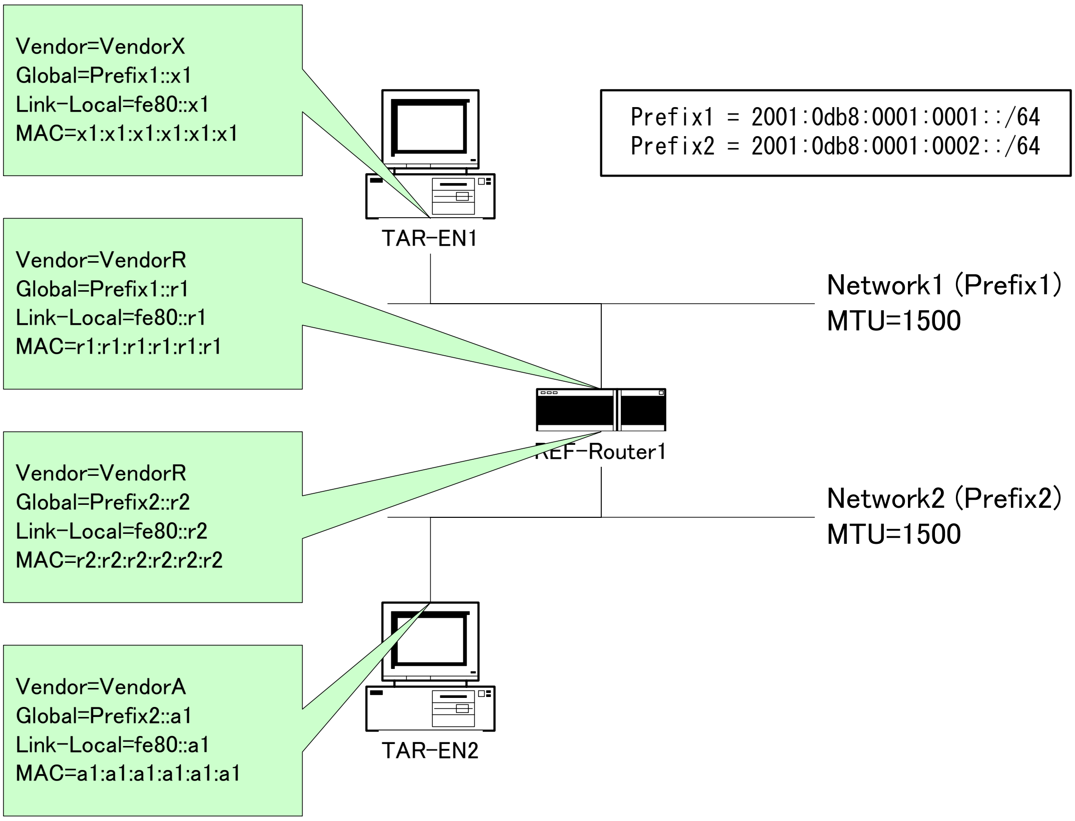


Fig 1 Topology figure example 1

```
    TAR-EN1
       |
   ----+-------+--- Network1
               |
          REF-Router1
               |
   ----+-------+--- Network2
       |
    TAR-EN2

Network1
========
    Prefix: 2001:db8:1:1::/64
    MTU: 1500

    TAR-EN1: VendorX
        Link-Local=fe80::x1
        Global=2001:db8:1:1::x1
        MAC=x1:x1:x1:x1:x1:x1

    REF-Router1: VendorR
        Link-Local=fe80::r1
        Global=2001:db8:1:1::r1
        MAC=r1:r1:r1:r1:r1:r1

Network2
========
    Prefix: 2001:db8:1:2::/64
    MTU: 1500

    REF-Router1: VendorR
        Link-Local=fe80::r2
        Global=2001:db8:1:2::r2
        MAC=r2:r2:r2:r2:r2:r2

    TAR-EN2: VendorA
        Link-Local=fe80::a1
        Global=2001:db8:1:2::a1
        MAC=a1:a1:a1:a1:a1:a1
```

Fig 2 Topology figure example 2

```
Network1
    Prefix: 2001:db8:1:1::/64
    MTU: 1500

Network2
    Prefix: 2001:db8:1:2::/64
    MTU: 1500

TAR-EN1: VendorX
    Network1)
        Link-Local=fe80::x1
        Global=2001:db8:1:1::x1
        MAC=x1:x1:x1:x1:x1:x1

REF-Router1: VendorR
    Network1)
        Link-Local=fe80::r1
        Global=2001:db8:1:1::r1
        MAC=r1:r1:r1:r1:r1:r1

    Network2)
        Link-Local=fe80::r2
        Global=2001:db8:1:2::r2
        MAC=r2:r2:r2:r2:r2:r2

TAR-EN2: VendorA
    Network2)
        Link-Local=fe80::a1
        Global=2001:db8:1:2::a1
        MAC=a1:a1:a1:a1:a1:a1
```

Fig 3 Address List example

Configuration File (Required)

Save the configuration information of IKEv2 function. This file must be able to indicate IKE_SA and CHILD_SA information. If the device is configured by the individual configuration file, the file itself can be used. If the device is configured by CUI, the typescript of terminal session can be used. If the device is configured by GUI, the screen capture can be used.

Command Log (Required)

Save the command files for each test on each node.

Packet Capture File (Required)

Capture all packets on each link during the test with a device that is not part of the test. For each part of test put the captured packet into individual files within tcpdump (pcap) format, or readable HTML format.

When you run tcpdump, please specify snap length as 4096 bytes.

e.g.,) tcpdump -i if0 -s 4096 -w 1.1.A.VendorA.Network1.dump

Test Result Table (Required)

Collect all test result tables in a file and fill the tables as required. This file must contain a table where all passes are clearly marked.

1.2. Data file name syntax

Please use following syntax in the file name.

A) Topology Map (Required)

Syntax: *Chapter.Section.Part.ON.topology*

For "ON", use the vendor name of the Node which behaved as a Opposite side target Node (ON).

e.g.,)

If your device is an End-Node, the name should be like following.

ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

1.1.A.VendorA.topology
1.1.B.VendorA.topology
1.1.E.VendorC.topology
1.1.F.VendorC.topology
1.12.A.VendorC.topology

If your device is a SGW, the name should be like following.

ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

1.1.C.VendorC.topology
1.1.D.VendorC.topology
1.12.A.VendorA.topology

B) Configuration File (Required)

Syntax: *Chapter.Section.Part.Device.conf*

For "ON" described below, use the vendor name of the Node which behaved as a Opposite side target Node (ON).

e.g.,)

When your vendor is VendorX and your device is an End-Node, the file name should be like following.

ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

1.1.A.VendorX.conf
1.1.A.VendorA.conf
1.1.B.VendorX.conf
1.1.B.VendorA.conf
1.1.E.VendorX.conf
1.1.E.VendorC.conf
1.1.F.VendorX.conf
1.1.F.VendorC.conf
1.12.A.VendorX.conf
1.12.A.VendorC.conf

When your vendor is VendorX and your device is a SGW, the file name should be like following.

ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

1.1.C.VendorX.conf
1.1.C.VendorC.conf
1.1.D.VendorX.conf
1.1.D.VendorC.conf
1.12.A.VendorX.conf
1.12.A.VendorA.conf

C) Command Log (Required)

Syntax: *Chapter.Section.Part.ON.result*

For "ON", use the vendor name of the Node which behaved as a Opposite side target Node (ON).

e.g.,)

If your device is an End-Node, the name should be like following.
ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]
ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

1.1.A.VendorA.result
1.1.B.VendorA.result
1.1.E.VendorC.result
1.1.F.VendorC.result
1.12.A.VendorC.result

If your device is a SGW, the name should be like following.
ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]
ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

1.1.C.VendorC.result
1.1.D.VendorC.result
1.12.A.VendorA.result

D) Packet Capture File (Required)

Syntax: *Chapter.Section.Part.ON.Network.dump*

For "*Network*", use the captured network name.

For "ON", use the vendor name of the Node which behaved as a Opposite side target Node (ON).

e.g.,)

If your device is an End-Node, the name should be like following.
ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]
ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]

1.1.A.VendorA.Network1.dump
1.1.A.VendorA.Network2.dump
1.1.B.VendorA.Network1.dump
1.1.B.VendorA.Network2.dump
1.1.E.VendorC.Network1.dump
1.1.E.VendorC.Network2.dump
1.1.E.VendorC.Network3.dump
1.1.F.VendorC.Network1.dump
1.1.F.VendorC.Network2.dump
1.1.F.VendorC.Network3.dump
1.12.A.VendorC.Network1.dump
1.12.A.VendorC.Network2.dump
1.12.A.VendorC.Network3.dump

If your device is a SGW, the name should be like following.
ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]
ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]

1.1.C.VendorC.Network1.result
1.1.C.VendorC.Network2.result
1.1.C.VendorC.Network3.result
1.1.C.VendorC.Network4.result
1.1.D.VendorC.Network1.result
1.1.D.VendorC.Network2.result
1.1.D.VendorC.Network3.result
1.1.D.VendorC.Network4.result
1.12.A.VendorA.Network1.result
1.12.A.VendorA.Network2.result
1.12.A.VendorA.Network3.result

E) Test Result Table (Required)

Syntax: *Target_Node.table*

In this file you should make table for each part.
Your device can be described hereafter as a sample whether it is a End-Node or a SGW.
ON: End-Node [vendor: VendorA, model: rEN1, version: 1.0]
ON: End-Node [vendor: VendorB, model: rEN2, version: 2.0]
ON: SGW [vendor: VendorC, model: rSGW1, version: 3.0]
ON: SGW [vendor: VendorD, model: rSGW2, version: 4.0]

For End-Node to End-Node tests, following table is required.

	VendorA	VendorB
VendorX		

For End-Node to SGW tests, following table is required. (If your device is a End-Node)

	VendorC	VendorD
VendorX		

For SGW to End-Node tests, following table is required. (If your device is a SGW)

	VendorA	VendorB
VendorX		

For SGW to SGW tests, following table is required.

	VendorC	VendorD
VendorX		

e.g.,)
Test result of following End-Node.
TAR-EN1: End-Node [vendor: VendorX, model: rEN1, version: 5.0]
or
Test result of following SGW.
TAR-SGW1: SGW [vendor: VendorX, model: rSGW1, version: 5.0]

VendorX.table

1.3. Data Archive

Please organize your data as following directory structure.

```
In the case of when your device is an End-Node)
        ${Your_Device_ver}/
                Conformance/
                Interoperability/
                        ${TAR-EN2_Vendor_Name_1}/
                        ${TAR-EN2_Vendor_Name_2}/
                        ${TAR-SGW1_Vendor_Name_1}/      (optional)
                        ${TAR-SGW1_Vendor_Name_2}/      (optional)

In the case of when your device is a SGW)
        ${Your_Device_ver}/
                Conformance/
                Interoperability/
                        ${TAR-SGW2_Vendor_Name_1}/
                        ${TAR-SGW2_Vendor_Name_2}/
                        ${TAR-EN1_Vendor_Name_1}/       (optional)
                        ${TAR-EN1_Vendor_Name_2}/       (optional)
```

Put all interoperability data file in "Interoperability" directory.
Put all Conformance Self-Test results or Conformance Lab test results in "Conformance" directory.
Make a tar.gz format archive file, and put files under "${Your_Device_ver}" in it.

1.4. Network Traffic Application

In the test results, "ping" is the default application to send ICMP echo request.

If the target device does not have "ping" application, it is possible to use any other application that behaves like the "ping" application and passes traffic through the network.

****