



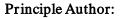
MODIFICATION RECORD

Version 1.11.0	May 10, 2011
	- Change test sequence of Section 5.3.11 (Section 5.3.11 uses new test topology For
	End-Node vs. SGW Tunnel Mode Test 2)
	- Removed NULL Authentication tests
	- Typos and Bug fixes
Version 1.10.0	May 31, 2010
	- Support Authentication Algorithm HMAC-SHA-256 in RFC 4868 (Using
	HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec) (Section
	5.1.12, 5.2.12, 5.3.12, 5.4.12)
Version 1.9.2	March 11, 2010
	- Add Fragmentation test cases (Section 5.1.11, 5.2.11, 5.3.11, 5.4.11)
	- Editorial fix at Appendix-A Section 1.2
	- Added the description of keying information file at Appendix-A Required Data
	- Added file lists needed to be submitted at Appendix-A Section 1.3
	- Clarified the interoperable device requirement at REQUIREMENTS section
Version 1.9.1	January 06, 2009
	- Support the passive node which doesn't have ping6 application (as Possible
	Problems in Section 5.1.8, 5.3.8, 5.4.8)
Version 1.9.0	December 09, 2008
	- Support RFC 4312 (The Camellia Cipher Algorithm and Its Use With IPsec)
	(Section 5.1.7, 5.2.7, 5.3.7, 5.4.7)
	- Use IPv6 prefix defined in RFC 3849 for the documentation
Version 1.5.2	October 11, 2007
	- Remove ESN test cases (Section 5.1.8, 5.2.8, 5.3.8, 5.4.8)
Version 1.5.1	June 19, 2007
	- Correct subsection in Section 5.3
Version 1.5.0	April 27, 2007
	- Support IPsec v3
Version 1.4.3	October 6, 2005
X7 : 1.40	- Update Appendix
Version 1.4.2	September 30, 2005
**	- Change ping direction for tunnel tests between END-Nodes
Version 1.4.1	September 22, 2005
X7 ' 1 4	- Editorial fix
Version 1.4	March 1, 2005
X7 : 10	- Change Keys
Version 1.3	December 21, 2004
W 1 0	- Correct Require table
Version 1.2	November 29, 2004
	- Add concept of End-Node rather than Host
	- Add criteria - Editorial fix
Version 1.1	
Version 1.1	September 30, 2004
version 1.0	September 24, 2004



ACKNOWLEDGMENTS

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



- TAHI Project

Commentators:

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



INTRODUCTION

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

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



The IPv6 Logo Program consists of three phases:

Phase 1:

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

Phase 2:

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

To avoid confusion, the logo "IPv6 Ready" will be generic. The v6RLC will define the test profiles with associated requirements for specific functionalities.

Phase 3:

Same as Phase 2 with IPsec mandated.



REQUIREMENTS

To obtain the IPv6 Ready Logo Phase-2 for IPsec (IPsec Logo), the Node Under Test (NUT) must satisfy following requirements.

Equipment Type:

We define following two equipment types. Every NUT can be ether of them.

End-Node:

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

SGW (Security Gateway):

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

Security Protocol:

NUT have to pass all the tests of ESP regardless the type of the NUT. The IPv6 Ready Logo Program does not focus on AH.

Mode:

The mode requirement depends on the type of NUT.

End-Node:

If the NUT is a End-Node, it have to pass all the tests of Transport mode. If the NUT supports the Tunnel mode, it also have to pass all the tests of Tunnel mode. (i.e., Tunnel mode is ADVANCED functionality for End-Node)

SGW:

If the NUT is a SGW, it has to pass all the test of Tunnel mode.



Encryption Algorithm:

IPv6 Logo Committee had defined BASE ALGORITHM and ADVANCED ALGORITHM. All NUT have to pass all the test of BASE ALGORITHM to obtain the IPsec Logo. The NUT which supports the algorithms that are listed as ADVANCED ALGORITHM, have to pass all the corresponding tests.

The algorithm requirement is independent from NUT type.

BASE ALGORITHM: 3DES-CBC

ADVANCED ALGORITHM:
AES-CBC
AES-CTR
NULL
CAMELLIA-CBC

Authentication Algorithm:

IPv6 Logo Committee had defined BASE ALGORITHM and ADVANCED ALGORITHM. All NUTs have to pass all the test of BASE ALGORITHM to obtain the IPsec Logo. The NUTs, which support the algorithms that are listed as ADVANCED ALGORITHM, have to pass all the corresponding tests.

The algorithm requirement is independent from NUT type.

BASE ALGORITHM: HMAC-SHA1

ADVANCED ALGORITHM: AES-XCBC-MAC-96 NULL HMAC-SHA-256



Category:

In this document, the tests are categorized into two types, BASIC and ADVANCED. ALL NUT are required to support BASIC. ADVANCED is required for all NUT which supports ADVANCED encryption/authentication algorithm. In each test description contains a Category section. The section lists the requirements to satisfy each test.

Interoperable device requirement:

IPv6 Logo Committee requires interoperable devices to obtain the IPv6 Ready Logo Phase-2 as following.

For End-Node:

Transport Mode (BASIC): Test 5.1.X is required. 2 End-Node devices from different vendors

Tunnel Mode (ADVANCED): Test 5.3.X or Test 5.4.X is required. 2 SGW devices or 2 End-Node devices from different vendors These 2 vendors must not be same as the vendors for transport mode test

Tost 5 1 V	est 5.1.X Transport Mode	End-Node 1	Vendor A	BASIC
Test J.1.A		End-Node 2	Vendor B	DASIC
Test 5.2 V Tunnal Made	Tunnal Mada	SGW 1	Vendor C	ADVANCED
Test 5.3.X Tunnel Mode		SGW 2	Vendor D	ADVANCED

or

Toot 5.1 V	Transport Mode	End-Node 1	Vendor A	BASIC	
Test 3.1.A	Transport Mode	End-Node 2	Vendor B	DASIC	
Test 5 4 V	Test 5 4 V Test al Mada	End-Node 3	Vendor C	ADVANCED	
Test 5.4.X Tunnel Mode		End-Node 4	Vendor D	ADVANCED	

For SGW:

Tunnel Mode (BASIC): Test 5.2.X or Test 5.3.X is required. 2 SGW devices or 2 End-Node devices from different vendors

Tost 5.2 V	Tunnel Mode	SGW 1	Vendor A	BASIC
16st 3.2.A	Tuillei Wiode	SGW 2	Vendor B	DASIC

or

Test 5.2 V	Tunnel Mode	End-Node 1	Vendor A	DACIC
Test 3.3.A	Tuillei Mode	End-Node 2	Vendor B	DASIC



REFERENCES

This test specification focus on the following IPsec related RFCs.

- [RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.
- [RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.
- [RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.
- [RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.
- [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.
- [RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- [RFC4305] Eastlake, D., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4305, December 2005.
- [RFC4312] A. Kato, S. Moriai, and M. Kanda, "The Camellia Cipher Algorithm and Its Use With IPsec", RFC 4312, December 2005.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.
- [RFC4868] S. Kelly, and S. Franke, "Using HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with IPsec", RFC4868, May 2007.

IPsec



TABLE OF CONTENTS

MO	DIFICATI	ON RECORD	1
ACI	KNOWLE	DGMENTS	2
INT	RODUCT	ION	3
REC	QUIREME	ENTS	5
REF	FERENCE	S	8
TAE	BLE OF C	ONTENTS	9
1.	Test Deta	ils	. 12
2.	Test Topo	ology	. 13
F	or End-N	ode vs. End-Node Transport/Tunnel Mode Test	. 13
F	or SGW v	s. SGW Tunnel Mode Test	. 14
F	or End-N	ode vs. SGW Tunnel Mode Test 1	. 15
F	or End-N	ode vs. SGW Tunnel Mode Test 2	. 16
3.	Descripti	on	. 17
4.	Required	Tests	. 18
5.	Test Scen	nario	. 21
5.	.1. Tran	sport Mode (End-Node vs. End-Node)	. 21
	5.1.1.	Transport Mode: ESP=3DES-CBC HMAC-SHA1	. 22
	5.1.2.	Transport Mode: ESP=3DES-CBC AES-XCBC	. 27
	5.1.3.	Transport Mode: ESP=3DES-CBC NULL	. 32
	5.1.4.	Transport Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	. 33
	5.1.5.	Transport Mode: ESP=AES-CTR HMAC-SHA1	. 38
	5.1.6.	Transport Mode: ESP=NULL HMAC-SHA1	. 43
	5.1.7.	Transport Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	. 48
	5.1.8.	Transport Mode: Select SPD (ICMP Type)	. 53
	5.1.9.	Transport Mode: dummy packet handling	. 61
	5.1.10.	Transport Mode: TFC padding	. 67
	5.1.11.	Transport Mode: Fragmentation	. 74
	5.1.12.	Transport Mode: ESP=3DES-CBC HMAC-SHA-256	. 81



5.2. T	unnel Mode (SGW vs. SGW)	86
5.2.1.	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	87
5.2.2.	Tunnel Mode: ESP=3DES-CBC AES-XCBC	93
5.2.3.	Tunnel Mode: ESP=3DES-CBC NULL	99
5.2.4.	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	100
5.2.5.	Tunnel Mode: ESP=AES-CTR HMAC-SHA1	106
5.2.6.	Tunnel Mode: ESP=NULL HMAC-SHA1	112
5.2.7.	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	118
5.2.8.	Tunnel Mode: Select SPD (ICMP Type)	124
5.2.9.	Tunnel Mode: dummy packet handling	133
5.2.10	Tunnel Mode: TFC padding	140
5.2.11.	Tunnel Mode: Fragmentation	147
5.2.12	Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256	157
5.3. T	unnel Mode (End-Node vs. SGW)	163
5.3.1.	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	164
5.3.2.	Tunnel Mode: ESP=3DES-CBC AES-XCBC	169
5.3.3.	Tunnel Mode: ESP=3DES-CBC NULL	174
5.3.4.	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	175
5.3.5.	Tunnel Mode: ESP=AES-CTR HMAC-SHA1	180
5.3.6.	Tunnel Mode: ESP=NULL HMAC-SHA1	185
5.3.7.	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	190
5.3.8.	Tunnel Mode: Select SPD (ICMP Type)	195
5.3.9.	Tunnel Mode: dummy packet handling	204
5.3.10	Tunnel Mode: TFC padding	211
5.3.11.	Tunnel Mode: Fragmentation	218
5.3.12	Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256	232
5.4. T	unnel Mode (End-Node vs. End-Node)	237
5.4.1.	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	238
5.4.2.	Tunnel Mode: ESP=3DES-CBC AES-XCBC	243
5.4.3.	Tunnel Mode: ESP=3DES-CBC NULL	248
5.4.4.	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	249



5.4.5.	Tunnel Mode: ESP=AES-CTR HMAC-SHA1254
5.4.6.	Tunnel Mode: ESP=NULL HMAC-SHA1
5.4.7.	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1 264
5.4.8.	Tunnel Mode: Select SPD (ICMP Type)
5.4.9.	Tunnel Mode: dummy packet handling
5.4.10.	Tunnel Mode: TFC padding
5.4.11.	Tunnel Mode: Fragmentation
5.4.12.	Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256
Appendix-A	Required Data
1.1. Rec	uired Data Type
1.2. Dat	a file name syntax
1.3. Dat	a Archive
Appendix-B	annex-5.1.8 for the passive node
1.1. usir	ng UDP application to invoke ICMPv6 Destination Unreachable (Port
unreachable	e)
1.2. invo	oking Neighbor Unreachability Detection
Appendix-C	annex-5.3.8 for the passive node
Appendix-D	annex-5.4.8 for the passive node
1.1. usir	ng UDP application to invoke ICMPv6 Destination Unreachable (Port
unreachable	e)
1.2. invo	oking Neighbor Unreachability Detection



1. Test Details

In this chapter, detail information, including terminology, is described.

Terminology:

ROUTER: A device which can forward the packets. HOST: A device which is not a ROUTER. End-Node: Host and Router can be an End-Node.

Security Gateway. SGW is a kind of ROUTER. SGW:

Required Application:

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

IPsec Configuration:

Manual key configuration is used by default and is a minimal requirement. IKE is an acceptable alternative to use when IPsec is tested. When IKE is used, the encryption key and authentication key are negotiated dynamically. In that case, dynamic keys are used rather than the static keys specified in this document. The tester should support the alternative of using IKE with dynamic keys to execute the tests.

Topology:

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



2. Test Topology

These logical Network Topologies are used for test samples.

For End-Node vs. End-Node Transport/Tunnel Mode Test

- 1. Set global address to TGT_HOST1_Link0 and TGT_HOST2_Link1 by RA.
- 2. Make IPsec transport mode or tunnel mode between TGT_HOST1 and TGT_HOST2.
- 3. For Fragmentation test (5.1.11 and 5.4.11), configure the Link1 interface on REF_ROUTER1 with a path MTU of 1280 byte.

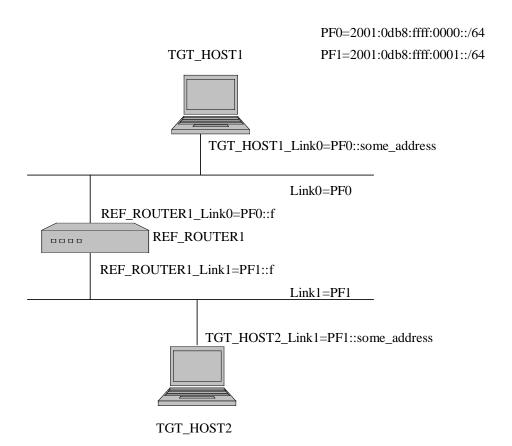


Figure 1 Topology for End-Node: Transport and Tunnel mode with End-Node



For SGW vs. SGW Tunnel Mode Test

- 1. Set global address to REF_HOST1_Link0 and REF_HOST2_Link3 by RA.
- 2. Set global address to TGT_SGW1_Link0, TGT_SGW1_Link1, TGT_SGW2_Link2, TGT_SGW2_Link3, REF_ROUTER1_Link1, REF_ROUTER1_Link2 manually.
- 3. Set routing table to TGT_SGW1 (REF_ROUTER1_Link1 for Link2 and Link3)
- 4. Set routing table to TGT_SGW2 (REF_ROUTER1_Link2 for Link0 and Link1)
- 5. Set routing table to REF_ROUTER1 (TGT_SGW1_Link1 for Link0, TGT_SGW2_Link2 for Link3)
- 6. Make IPsec tunnel mode between TGT_SGW1 and TGT_SGW2.
- 7. For 5.2.11 Fragmentation test, configure the Link2 interface on REF_ROUTER1 and TGT_SGW2 with a path MTU of 1280 byte.

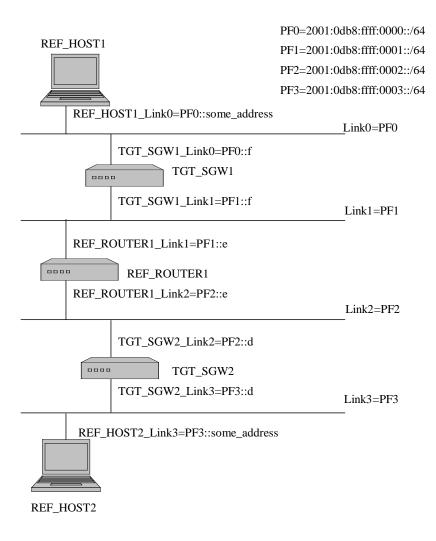


Figure 2 Topology for SGW: Tunnel mode with SGW



For End-Node vs. SGW Tunnel Mode Test 1

- 1. Set global address to TGT_HOST1_Link0 and REF_HOST2_Link2 by RA.
- 2. Set global address to TGT_SGW1_Link1 and TGT_SGW1_Link2 manually.
- 3. Set routing table to TGT_SGW1 (REF_ROUTER1_Link1 for Link0)
- 4. Set routing table to REF_ROUTER1 (TGT_SGW1_Link1 for Link2)
- 5. Make IPsec tunnel mode between TGT_HOST1 and TGT_SGW1.

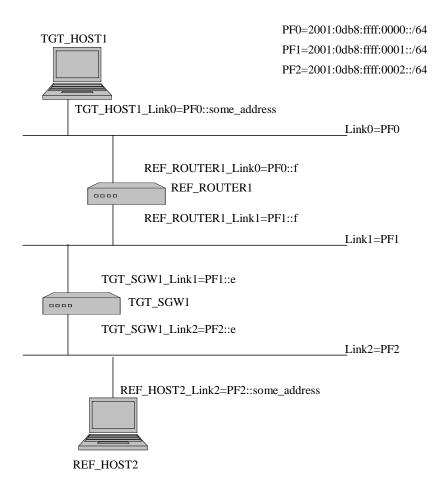


Figure 3 Topology for End-Node: Tunnel mode with SGW



For End-Node vs. SGW Tunnel Mode Test 2

- 1. Set global address to TGT_HOST1_Link0 and REF_HOST2_Link2 by RA.
- 2. Set global address to TGT_SGW1_Link1 and TGT_SGW1_Link2 manually.
- 3. Set routing table to TGT_SGW1 (REF_ROUTER1_Link1 for Link0)
- 4. Set routing table to REF_ROUTER1 (TGT_SGW1_Link1 for Link2)
- 5. Make IPsec tunnel mode between TGT_HOST1 and TGT_SGW1.

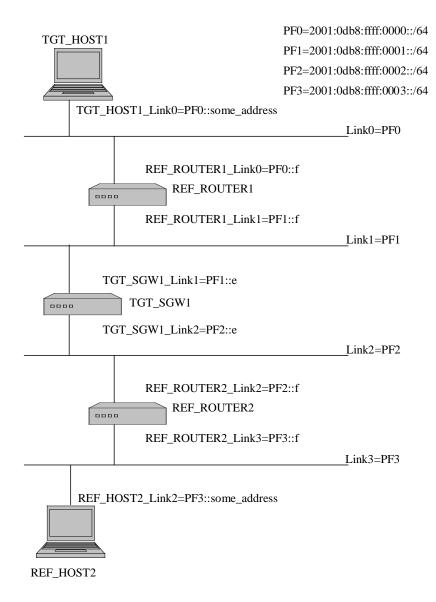


Figure 4 Topology for End-Node: Tunnel mode with SGW



3. Description

Each test scenario consists of following parts.

Purpose: The Purpose is the short statement describing what the test attempts to achieve.

It is usually phrased as a simple assertion of the future or capability to be tested.

Category: The Category shows you who need to satisfy the test shortly.

References: Reference RFC list containing description related to the test.

Initialization: The Initialization describes how to initialize and configure the NUT before

starting each test. If a value is not provided, then the protocol's default value is

used.

Packets: The Packets describes the simple figure of packets which is used in the test. In

this document, the packet name is represented in Italic style font.

Procedure: The Procedure describes step-by-step instructions for carrying out the test.

Judgment: The Judgment describes expected result. If we can observe as same result as the

description of Judgment, the NUT passes the test.

Possible Problems: This section contains a description of known issues with the test procedure,

which may affect test results in certain situations.



4. Required Tests

The following table describes which tests are required.

Focused Interface	Test Title	Device Type	Device Type		
		End-Node	SGW		
End-Node vs. End-Node	5.1.1 Transport Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	N/A		
(Transport)	5.1.2 Transport Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	N/A		
	5.1.3 Transport Mode: ESP=3DES CBC NULL	ADVANCED	N/A		
	5.1.4 Transport Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A		
	5.1.5 Transport Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	N/A		
	5.1.6 Transport Mode: ESP=NULL HMAC-SHA1	ADVANCED	N/A		
	5.1.7 Transport Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A		
	5.1.8 Transport Mode: Select SPD (ICMP Type)	ADVANCED *3	N/A		
	5.1.9 Transport Mode: dummy packet handling	ADVANCED	N/A		
	5.1.10 Transport Mode: TFC padding	ADVANCED *4	N/A		
	5.1.11 Transport Mode : Fragmentation	BASIC	N/A		
	5.1.12 Transport Mode: ESP=3DES-CBC HMAC-SHA-256	ADVANCED	N/A		
SGW vs. SGW (Tunnel)	5.2.1 Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	N/A	BASIC		
*1	5.2.2 Tunnel Mode: ESP=3DES-CBC AES-XCBC	N/A	ADVANCED		
	5.2.3 Tunnel Mode: ESP=3DES CBC NULL	N/A	ADVANCED		
	5.2.4 Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	N/A	ADVANCED		
	5.2.5 Tunnel Mode: ESP=AES-CTR HMAC-SHA1	N/A	ADVANCED		
	5.2.6 Tunnel Mode: ESP=NULL HMAC-SHA1	N/A	ADVANCED		
	5.2.7 Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	N/A	ADVANCED		
	5.2.8 Tunnel Mode: ESP=Select SPD (ICMP Type)	N/A	ADVANCED *3		
	5.2.9 Tunnel Mode: ESP=dummy packet	N/A	ADVANCED		
	5.2.10 Tunnel Mode: ESP=TFC padding	N/A	ADVANCED		
	5.2.11 Tunnel Mode : Fragmentation	N/A	BASIC		
	5.2.12 Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256	N/A	ADVANCED		



Focused Interface	Test Title	Device Type	
		End-Node	SGW
End-Node vs. SGW	5.3.1 Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	BASIC
(Tunnel)	5.3.2 Tunnel Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	ADVANCED
*1, *2	5.3.3 Tunnel Mode: ESP=3DES CBC NULL	ADVANCED	ADVANCED
	5.3.4 Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	ADVANCED
	5.3.5 Tunnel Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	ADVANCED
	5.3.6 Tunnel Mode: ESP=NULL HMAC-SHA1	ADVANCED	ADVANCED
	5.3.7 Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	ADVANCED
	5.3.8 Tunnel Mode: ESP=Select SPD (ICMP Type)	ADVANCED *3	ADVANCED *3
	5.3.9 Tunnel Mode: ESP=dummy packet handling	ADVANCED	ADVANCED
	5.3.10 Tunnel Mode: ESP=TFC padding	ADVANCED	ADVANCED
	5.3.11 Tunnel Mode : Fragmentation	BASIC	BASIC
	5.3.12 Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256	ADVANCED	ADVANCED
End-Node vs. End-Node	5.4.1 Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	N/A
(Tunnel)	5.4.2 Tunnel Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	N/A
*1, *2	5.4.3 Tunnel Mode: ESP=3DES CBC NULL	ADVANCED	N/A
	5.4.4 Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	5.4.5 Tunnel Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	N/A
	5.4.6 Tunnel Mode: ESP=NULL HMAC-SHA1	ADVANCED	N/A
	5.4.7 Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	5.4.8 Tunnel Mode: ESP=Select SPD (ICMP Type)	ADVANCED *3	N/A
	5.4.9 Tunnel Mode: ESP=dummy packet handling	ADVANCED	N/A
	5.4.10 Tunnel Mode: ESP=TFC padding	ADVANCED	N/A
	5.4.11 Tunnel Mode : Fragmentation	BASIC	
	5.4.12 Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256	ADVANCED	N/A



- *1: If applicant's device is a SGW, either of them ("SGW vs. SGW" or "End-Node vs. SGW") must be run. Applicants need to run test with more than 2 implementations as a counter part regardless equipment type. The case you choose SGW as a counter part, you need to run the test of "SGW vs. SGW". The case you choose End-Node as a counter part, you need to run the test of "End-Node vs. SGW".
- *2: If applicant's device is an End-Node and it supports Tunnel Mode, either of them must be run.

 Applicants need to run test with more than 2 implementations as a counter part regardless equipment type. The case you choose SGW as a counter part, you need to run the test of "End-Node vs. SGW". The case you choose End-Node as a counter part, you need to run the test of "End-Node vs. End-Node".
- *3: This test should be done by using ICMP.
- *4: This test should be done by using UDP.



5. Test Scenario

This Chapter consists of following 4 sections of test scenarios.

- Transport Mode (End-Node vs. End-Node)
- Tunnel Mode (End-Node vs. End-Node)
- Tunnel Mode (End-Node vs. SGW)
- Tunnel Mode (SGW vs. SGW)

5.1. Transport Mode (End-Node vs. End-Node)

Scope:

Following tests focus on Transport Mode.

Overview:

Tests in this section verify that a node properly processes and transmits the packets to which IPsec Transport Mode is applied between two End-Nodes.



5.1.1. Transport Mode: ESP=3DES-CBC HMAC-SHA1

Purpose:

Transport mode between two End-Nodes, ESP=3DES-CBC HMAC-SHA1

Category:

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

SGW : N/A

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HC	OST1
HOST2_SA-0	·>	HOST1_	_SA-I
HOST2_SA-I <		HOST1_	SA-0



Security Association Database (SAD) for HOST1_SA-I

(Cook 12) //Cook 141/01/ Patabacc (C	, ioi iiooi i_oii i
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

•	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

Total Total Table Table Table Total Total Table	
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

	-
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

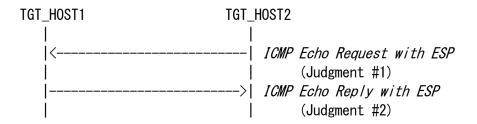
,		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.2. Transport Mode: ESP=3DES-CBC AES-XCBC

Purpose:

Transport mode between two End-Nodes, ESP=3DES-CBC AES-XCBC

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC

as an authentication algorithm)

SGW : N/A

References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOS	ST1
HOST2_SA-0	>	HOST1	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1 SA-I

deddirey hooderacter bacasade (ons) for hooti-on i		
TGT_HOST2_Link1		
TGT_HOST1_Link0		
0x1000		
transport		
ESP		
3DES-CBC		
ipv6readylogo3descbc2to1		
AES-XCBC-MAC-96		
ipv6readaesx2to1		

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

` `	· <u>=</u>
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

•	—
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

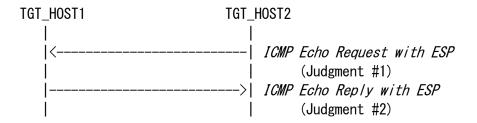
zem zeme megaeee		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	AES-XCBC-MAC-96
	Authentication Key	ipv6readaesx2to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_H0ST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	AES-XCBC-MAC-96
	Authentication Key	ipv6readaesx1to2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.3. Transport Mode: ESP=3DES-CBC NULL

D		
Pur	pose	

Transport mode between two End-Nodes, ESP=3DES-CBC NULL

Removed at revision 1.11.0.



5.1.4. Transport Mode: ESP=AES-CBC(128-bit) HMAC-SHA1

Purpose:

Transport mode between two End-Nodes, ESP-AES-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

AES-CBC(128-bit) as an encryption algorithm)

SGW : N/A

References:

- [RFC2404]
- [RFC2451]
- [RFC3602]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_H0ST2		TGT_HO	ST1
H0ST2_SA-0	>	HOST1	_SA-I
HOST2_SA-I <		HOST1	_SA-0



Security Association Database (SAD) for HOST1_SA-I

Total 10, Modern Bacasace (SMB) 101 Mod 1_0M 1	
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for $HOST1_SA-0$

source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

• • • • • • • • • • • • • • • • • • • •	-
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC (128-bit)
ESP key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

	—
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC (128-bit)
ESP key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

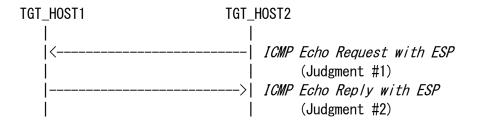
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	KEY	ipv6readaesc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CBC(128-bit)
	KEY	ipv6readaesc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. Otherwise, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.5. Transport Mode: ESP=AES-CTR HMAC-SHA1

Purpose:

Transport mode between two End-Nodes, ESP=AES-CTR HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-CTR

as an encryption algorithm)

: N/A SGW

References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1_SA-I

Total 10, Modern Business (CMB) 101 Mod 1_CM 1			
source address	TGT_HOST2_Link1	TGT_H0ST2_Link1	
destination address	TGT_HOST1_Link0		
SPI	0x1000		
mode	transport		
protocol	ESP		
ESP algorithm	AES-CTR		
ESP key	ipv6readylogoaes2to1		
ESP authentication	HMAC-SHA1		
ESP authentication key ipv6readylogsha12to1			

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	transport	

Security Association Database (SAD) for HOST1_SA-0

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST1_LinkO
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP key	ipv6readylogoaes1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key ipv6readylogsha11to2		

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

,		
source address	TGT_H0ST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP key	ipv6readylogoaes2to1	
ESP authentication HMAC-SHA1		
ESP authentication key ipv6readylogsha12to1		

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

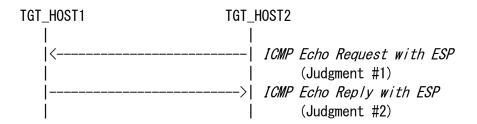
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CTR
	KEY	ipv6readylogoaes2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_H0ST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	KEY	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.6. Transport Mode: ESP=NULL HMAC-SHA1

Purpose:

Transport mode between two End-Nodes, ESP=NULL HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support NULL as

an encryption algorithm)

: N/A SGW

References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOS	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1 SA-I

Cocal Tey Medociae for Bacabaco (CMB) Tot Medit_OM 1		
TGT_HOST2_Link1		
TGT_HOST1_Link0		
0x1000		
transport		
ESP		
NULL		
HMAC-SHA1		
ipv6readylogsha12to1		

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

* * *	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy $\underline{\text{Database (SPD)}}$ for $\underline{\text{HOST1_SA-0}}$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

Total Tel Medicine Business (GMB) Tel Mediz_GM I		
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	NULL	
ESP key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

•	=
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

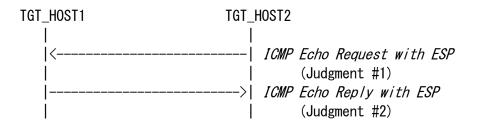
20111 20110 110441000 1111011 201		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	NULL
	KEY	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	NULL
	KEY	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. Otherwise, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.7. Transport Mode: ESP=CAMELLIA-CBC(128-bit) **HMAC-SHA1**

Purpose:

Transport mode between two End-Nodes, ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

CAMELLIA-CBC(128-bit) as an encryption algorithm)

SGW : N/A

References:

- [RFC2404]

- [RFC2451]

- [RFC4301]

- [RFC4303]

- [RFC4305]

- [RFC4312]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2	·	TGT_HOS	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	_SA-0



Security Association Database (SAD) for HOST1_SA-I

order (a) Modern Burdande (a) Por Modern_and I				
source address	TGT_HOST2_Link1			
destination address	TGT_HOST1_Link0			
SPI	0x1000			
mode	transport			
protocol	ESP			
ESP algorithm	CAMELLIA-CBC(128-bit)			
ESP key	ipv6readcamc2to1			
ESP authentication	HMAC-SHA1			
ESP authentication key	ipv6readylogsha12to1			

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	Any
direction	In
protocol	ESP
mode	Transport

Security Association Database (SAD) for HOST1_SA-0

•	—
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	Any
direction	Out
protocol	ESP
mode	Transport



Security Association Database (SAD) for HOST2_SA-I

order (a) Modern Burdando (a) Por Modern				
source address	TGT_HOST1_Link0			
destination address	TGT_H0ST2_Link1			
SPI	0x2000			
mode	Transport			
protocol	ESP			
ESP algorithm	CAMELLIA-CBC(128-bit)			
ESP key	ipv6readcamc1to2			
ESP authentication	HMAC-SHA1			
ESP authentication key	ipv6readylogsha11to2			

Security Policy Database (SPD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	Any
direction	In
protocol	ESP
mode	Transport

Security Association Database (SAD) for HOST2_SA-0

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	Transport
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	Any
direction	Out
protocol	ESP
mode	Transport



Packets:

ICMP Echo Request with ESP

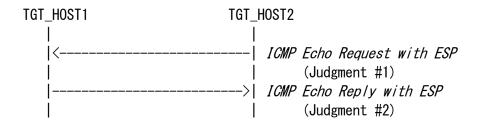
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	CAMELLIA-CBC(128-bit)
	KEY	ipv6readcamc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	KEY	ipv6readcamc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. Otherwise, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.1.8. Transport Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that can select ICMP

Type as SPD selector)

SGW : N/A

References:

- [RFC4301]
- [RFC4303]
- [RFC4443]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOST1			
HOST2_SA1-0	>	HOST1_SA1-	·I ICMPv6	Echo	Request
HOST2_SA1-I <		HOST1_SA1-	0 ICMPv6	Echo	Request
H0ST2_SA2-0	>	HOST1_SA2-	·I ICMPv6	Echo	Reply
HOST2 SA2-I <		HOST1 SA2-	0 ICMPv6	Echo	Reply



Security Association Database (SAD) for HOST1 SA1-I

TGT_HOST2_Link1
TGT_H0ST1_Link0
0x1000
transport
ESP
3DES-CBC
ipv6readylogo3des2to1req
HMAC-SHA1
ipv6readysha12to1req

Security Policy Database (SPD) for $HOST1_SA1-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA1-0

•	—
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST1_SA1-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2 SA1-I

TGT_HOST1_Link0
TGT_HOST2_Link1
0x2000
transport
ESP
3DES-CBC
ipv6readylogo3des1to2req
HMAC-SHA1
ipv6readysha11to2req

Security Policy Database (SPD) for $HOST2_SA1-I$

source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for $HOST2_SA1-0$

· · · · · · · · · · · · · · · · · · ·	
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1req

Security Policy Database (SPD) for TGT_HOST2_SA1-0

source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST1_SA2-I

total ity motoriation batabase (e	7.157 1 110 0 1 1 _ 0 7 1 _ 1
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD) for HOST1_SA2-I

source address	TGT_H0ST2_Link1
destination address	TGT_H0ST1_Link0
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA2-0

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST1_LinkO
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST1_SA2-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA2-I

occurred hereafter bacasace (one) for heart_one i		
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x4000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3des1to2rep	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha11to2rep	

Security Policy Database (SPD) for HOST2_SA2-I

source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA2-0

•	_
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD) for TGT_HOST2_SA2-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP1

20m Lone Reduces With Lori		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_LinkO
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP1

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Type	129 (Echo Reply)

ICMP Echo Request with ESP2

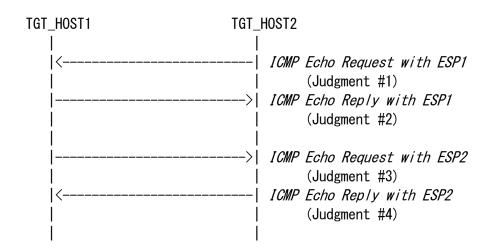
Tom Lone Request with Lorz		
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP2

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
ICMP	Туре	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP1" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP1"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2
- 6. TGT_HOST1 sends "ICMP Echo Request with ESP2" to TGT_HOST2
- 7. Observe the packet transmitted by TGT_HOST1
- 8. TGT_HOST2 sends "ICMP Echo Reply with ESP2"
- 9. Observe the packet transmitted by TGT_HOST2
- 10. Save the command log on TGT_HOST1



Judgment:

Judgment #1
Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP1"
Judgment #2
Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP1"
Judgment #3
Step-7: TGT_HOST1 transmits "ICMP Echo Request with ESP2"
Judgment #4
Step-9: TGT_HOST2 transmits "ICMP Echo Reply with ESP2"

Possible Problems:

TGT_HOST1 or TGT_HOST2 may be a passive node which does not implement an application for sending Echo Requests. One of the following method to perform this test is required for the passive node.

- a) using UDP application to invoke ICMPv6 Destination Unreachable (Port unreachable) (see Appendix-B Section 1.1)
- b) invoking Neighbor Unreachability Detection (see Appendix-B Section 1.2)



5.1.9. Transport Mode: dummy packet handling

Purpose:	
----------	--

Verify that device can handle dummy packet as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs

that support dummy packet handling)

SGW : N/A

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for HOST1 SA-I

occurred hoccorderon bacasace (one) for hocking.		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

•	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2 SA-I

Cocal Tey Moderation Bacasaco (CMB) Tot Modification 1		
TGT_HOST1_Link0		
TGT_HOST2_Link1		
0x2000		
transport		
ESP		
3DES-CBC		
ipv6readylogo3descbc1to2		
HMAC-SHA1		
ipv6readylogsha11to2		

Security Policy Database (SPD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

	-
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	0ut
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

zem zeme megaeee		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)

dummy packet 1

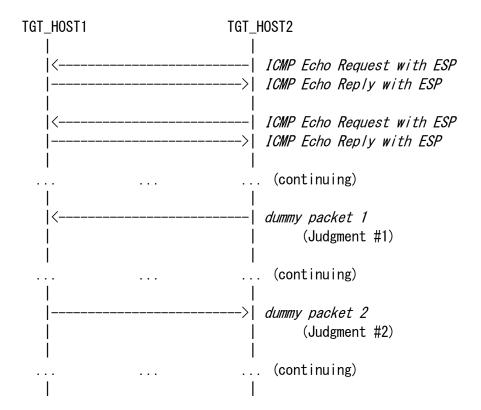
daning paonot i		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	Next Header	59 (no next header)

dummy packet 2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	Next Header	59 (no next header)



Procedure:



- 1. TGT_HOST2 keeps sending "ICMP Echo Request with ESP" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "dummy packet 1"

Judgment #2

Step-3: TGT_HOST1 transmits "dummy packet 2

Possible Problems:

None.



5.1.10. Transport Mode: TFC padding

Purpose	:

Verify that device can handle TFC padding as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support TFC padding)

SGW : N/A

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for HOST1_SA-I

Total 125 Moode action Business (only 101 Mootingon 1		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2 SA-I

110012_0/(1
TGT_HOST1_Link0
TGT_HOST2_Link1
0x2000
transport
ESP
3DES-CBC
ipv6readylogo3descbc1to2
HMAC-SHA1
ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST2_SA-I$

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	0ut
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)



ICMP Echo Request with TFC padded ESP

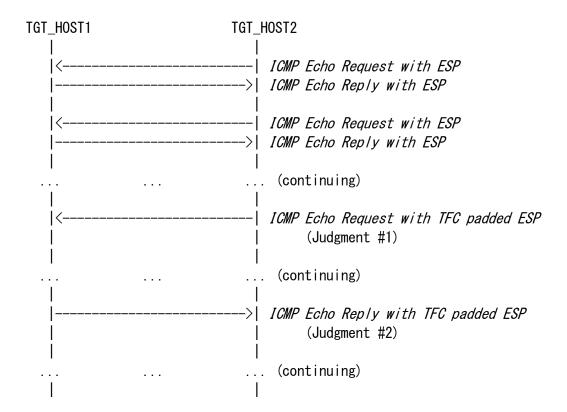
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with TFC padded ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	TFC padding	any size other than 0 bite
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 keeps sending "ICMP Echo Request with ESP" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with TFC padded ESP"

Judgment #2

Step-3: TGT_HOST1 transmits "ICMP Echo Reply with TFC padded ESP"

Possible Problems:

None.



5.1.11. Transport Mode: Fragmentation

Purpose:

Verify that device can handle ICMPv6 Error Message (Packet Too Big) and packet fragmentation/reassembly.

Category:

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

SGW : N/A

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_H	OST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	SA-0



Security Association Database (SAD) for HOST1_SA-I

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	Transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	Any
direction	In
protocol	ESP
mode	transport

Security Association Database (SAD) for $HOST1_SA-0$

·	—
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
upper spec	any	
direction	in	
protocol	ESP	
mode	transport	

Security Association Database (SAD) for $HOST2_SA-0$

•	—
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	Transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

Fragmented ICMP Echo Request with ESP 1

IP Header Source Address		TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

Fragmented ICMP Echo Request with ESP 2

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
	Payload Length	1460
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)

ICMP Error Message (Packet Too Big)

IP Header	Source Address	REF_ROUTER1
	Destination Address	TGT_HOST1
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply with
		ESP



Fragmented ICMP Echo Reply with ESP 1

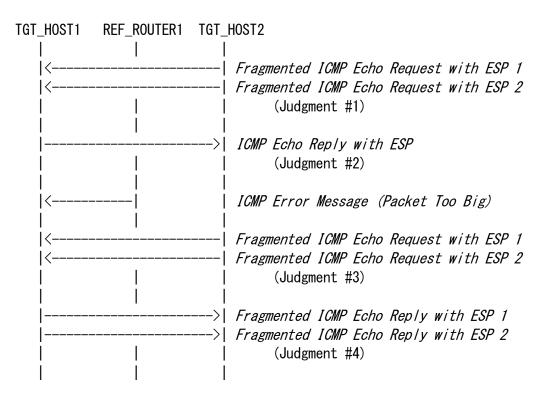
		TGT_HOST1_Link0
		TGT_HOST2_Link1
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Туре	129 (Echo Reply)

Fragmented ICMP Echo Reply with ESP 2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply



Procedure:



- 1. TGT_HOST2 transmits "Fragmented ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted by TGT HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. TGT HOST2 transmits "Fragmented ICMP Echo Request" to TGT HOST1
- 5. Observe the packet transmitted by TGT_HOST2
- 6. Observe the packet transmitted by TGT_HOST1
- 7. Save the command log on TGT_HOST2
- Disconnect TGT_HOST1 and TGT_HOST2. Connect TGT_HOST2 to LinkO. Connect TGT_HOST1 to Link1. Switch the roles of TGT_HOST1 and TGT_HOST2. Repeat step 1 to step 7

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "Fragmented ICMP Echo Request with ESP"

Judgment #2

Step-3: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Judgment #3

Step-5: TGT_HOST2 transmits "Fragmented ICMP Echo Request with ESP"

Judgment #4

 ${\tt Step-6: TGT_HOST1 \ transmits} \ \textit{``Fragmented ICMP Echo Reply with ESP''}$

Possible Problems:

None.



5.1.12. Transport Mode: ESP=3DES-CBC HMAC-SHA-256

Purpose:

Transport mode between two End-Nodes, ESP=3DES-CBC HMAC-SHA-256

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support

HMAC-SHA-256 as an authentication algorithm)

SGW : N/A

References:

- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4868]

Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

TGT_HOST2	Т	ΓGT_HO	ST1
HOST2_SA-0	> H	10ST1_	SA-I
HOST2 SA-I <	H	HOST1	SA-0



Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA-256	
ESP authentication key	ipv6readylogoph2ipsecsha22562to1	

Security Policy Database (SPD) for $HOST1_SA-I$

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST1_SA-0

TGT_HOST1_Link0
TGT_HOST2_Link1
0x2000
transport
ESP
3DES-CBC
ipv6readylogo3descbc1to2
HMAC-SHA-256
ipv6readylogoph2ipsecsha22561to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	transport



Security Association Database (SAD) for HOST2_SA-I

Total 10) Notice of a classic of (only) 101 Notice of 1		
source address	TGT_HOST1_Link0	
destination address	TGT_H0ST2_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA-256	
ESP authentication key	ipv6readylogoph2ipsecsha22561to2	

Security Policy Database (SPD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for HOST2_SA-0

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA-256	
ESP authentication key	ipv6readylogoph2ipsecsha22562to1	

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	transport



Packets:

ICMP Echo Request with ESP

20.00 100 100 100 100 100 100 100 100 100		
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha22562to1
ICMP	Type	128 (Echo Request)

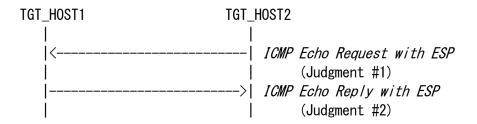
ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha22561to2
ICMP	Type	129 (Echo Reply)

84



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.2. Tunnel Mode (SGW vs. SGW)

Scope:

Following tests focus on Tunnel Mode between SGW and SGW.

Overview:

Tests in this section verify that a node properly processes and transmits the packets to which IPsec Tunnel Mode is applied between two SGWs.



5.2.1. Tunnel Mode: ESP=3DES-CBC HMAC-SHA1

Pu	rn	n	s	e	
		•	·	v	

Tunnel mode between two SGWs, ESP=3DES-CBC HMAC-SHA1

Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs if you choose SGW vs. SGW Tunnel

mode)

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

Total Tey house taction bacasass (Shb) Tot Saint_Sh 1		
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for SGW1_SA-I

Tunnel source address	TGT_SGW2_Link2	
Tunnel destination address	TGT_SGW1_Link1	
source address	Link3	
destination address	Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for SGW1_SA-0

•	·
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1	
Tunnel destination address	TGT_SGW2_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	Out	
protocol	ESP	
mode	tunnel	



Security Association Database (SAD) for SGW2_SA-I

source address	TGT_SGW1_Link1		
destination address	TGT_SGW2_Link2		
SPI	0x2000		
mode	tunnel		
protocol	ESP		
ESP algorithm	3DES-CBC		
ESP key	ipv6readylogo3descbc1to2		
ESP authentication HMAC-SHA1			
ESP authentication key ipv6readylogsha11to2			

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2	
Tunnel destination address	TGT_SGW1_Link1	
source address	Link3	
destination address	Link0	
upper spec	any	
direction	Out	
protocol	ESP	
mode	tunnel	



Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

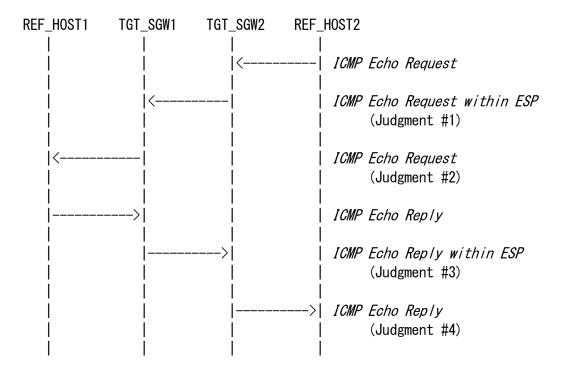
IP Header	Source Address	REF_H0ST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.2. Tunnel Mode: ESP=3DES-CBC AES-XCBC

Purpose	
rui puse	•
-	

Tunnel mode between two SGWs, ESP=3DES-CBC AES-XCBC

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-XCBC as an

authentication algorithm if you choose SGW vs. SGW Tunnel Mode)

References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1 SA-I

Total Tel Tacabaco (OND) Tot Call 1_ON 1	
TGT_SGW2_Link2	
TGT_SGW1_Link1	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbc2to1	
AES-XCBC	
ipv6readaesx2to1	

Security Policy Database (SPD) for SGW1_SA-I

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

TGT_SGW1_Link1
TGT_SGW2_Link2
0x2000
tunnel
ESP
3DES-CBC
ipv6readylogo3descbc1to2
AES-XCBC
ipv6readaesx1to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2 SA-I

Total Tey Moderation Bucusade (CMB) Tot Guile_GM 1	
TGT_SGW1_Link1	
TGT_SGW2_Link2	
0x2000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbc1to2	
AES-XCBC	
ipv6readaesx1to2	

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

	<u> </u>
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

zem zeme megaeee		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx2to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

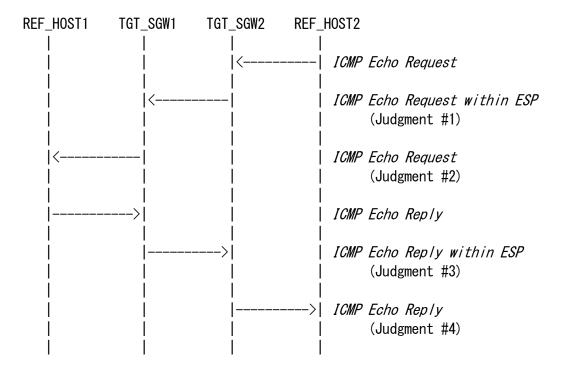
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx1to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.3. Tunnel Mode: ESP=3DES-CBC NULL

Tunnel mode between two SGWs, ESP=3DES-CBC NULL

Removed at revision 1.11.0.



5.2.4. Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between two SGWs, ESP=AES-CBC(128-bit) HMAC-SHA1

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CBC (128-bit)

as an encryption algorithm if you choose SGW vs. SGW Tunnel Mode)

References:

- [RFC2404]
- [RFC2451]
- [RFC3602]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1 SA-I

resident to the second	· • • • • • • • • • • • • • • • • • • •
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW1_SA-I$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

·	—
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

(0,12)	10. 04.12_0/. 1
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

TGT_SGW2_Link2
TGT_SGW1_Link1
0x1000
tunnel
ESP
AES-CBC(128-bit)
ipv6readaesc2to1
HMAC-SHA1
ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

zem zeme megaeee		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaesc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

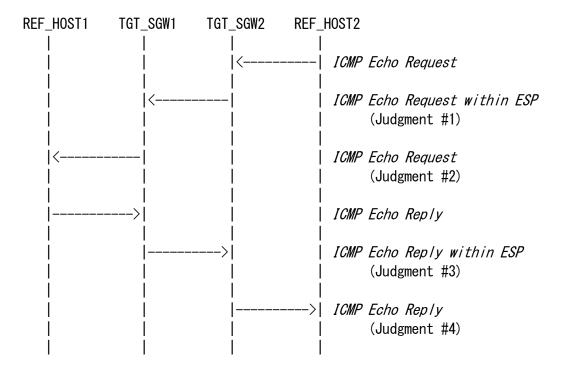
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	AES-CBC (128-bit)
	Key	ipv6readaesc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.5. Tunnel Mode: ESP=AES-CTR HMAC-SHA1

Pi	п	'n	'n	e	_	٠
	u	L	v	o	┖	•

Tunnel mode between two SGWs, ESP=AES-CTR HMAC-SHA1

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CTR as an

encryption algorithm if you choose SGW vs. SGW Tunnel Mode)

References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1 SA-I

Total Tey house the train bacasace (ons) for can 1_on 1		
TGT_SGW2_Link2		
TGT_SGW1_Link1		
0x1000		
tunnel		
ESP		
AES-CTR		
ipv6readylogoaes2to1		
HMAC-SHA1		
ipv6readylogsha12to1		

Security Policy Database (SPD) for $SGW1_SA-I$

TGT_SGW2_Link2
TGT_SGW1_Link1
Link3
Link0
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

· · · · · · · · · · · · · · · · · · ·	
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

total reg //occorderon business (one, remaining on i	
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW2_SA-I

T 1	TOT COMM I' I I
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

TGT_SGW2_Link2
TGT_SGW1_Link1
0x1000
tunnel
ESP
AES-CTR
ipv6readylogoaes2to1
HMAC-SHA1
ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

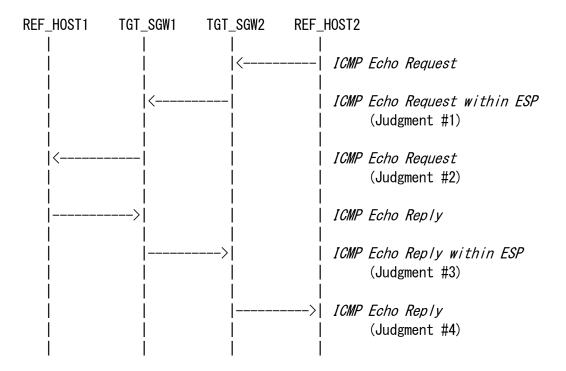
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

Tunnel mode between two SGWs, ESP=NULL HMAC-SHA1

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an

encryption algorithm are required to satisfy if you choose SGW vs.

SGW Tunnel Mode)

References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

Total 12) Modernation Business (ens.) 101 Cum _cm		
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for SGW1_SA-I

TGT_SGW2_Link2
TGT_SGW1_Link1
Link3
Link0
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunne
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

Total 10, Model at the Batanace (one, 10, canz_on 1	
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT SGW1 Link1
Turirie i source address	TUT_SUWT_LITIKT
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

zom zomo mogaco z		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

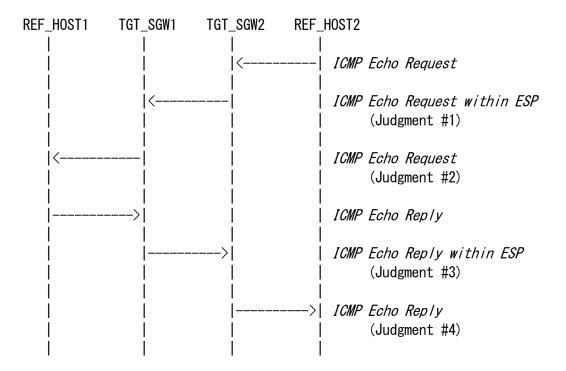
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.7. Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between two SGWs, ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support

CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose SGW

vs. SGW Tunnel Mode)

References:

- [RFC2404]

- [RFC2451]

- [RFC4301]

- [RFC4303]

- [RFC4305]

- [RFC4312]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

Todal 123 Notice at the Database (OND) 101 Cant_ON 1	
TGT_SGW2_Link2	
TGT_SGW1_Link1	
0x1000	
tunnel	
ESP	
CAMELLIA-CBC(128-bit)	
ipv6readcamc2to1	
HMAC-SHA1	
ipv6readylogsha12to1	

Security Policy Database (SPD) for SGW1_SA-I

TGT_SGW2_Link2
TGT_SGW1_Link1
Link3
Link0
Any
In
ESP
Tunnel

Security Association Database (SAD) for SGW1_SA-0

·	—
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	Tunne I
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Security Association Database (SAD) for SGW2_SA-I

codi i cy i i codo i de i con parabaco (crib)	101 04112_071 1
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	Tunne I
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW2_SA-I

T 1	TOT COMM I' I I
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	Any
direction	In
protocol	ESP
mode	Tunnel

Security Association Database (SAD) for SGW2_SA-0

Total 12) Moodo Tablo Dababase (emb) 101 Camb_on C		
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	Tunne I	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP key	ipv6readcamc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	
ESP algorithm ESP key ESP authentication	CAMELLIA-CBC(128-bit) ipv6readcamc2to1 HMAC-SHA1	

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	CAMELLILA-CBC(128-bit)
	Key	ipv6readcamc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

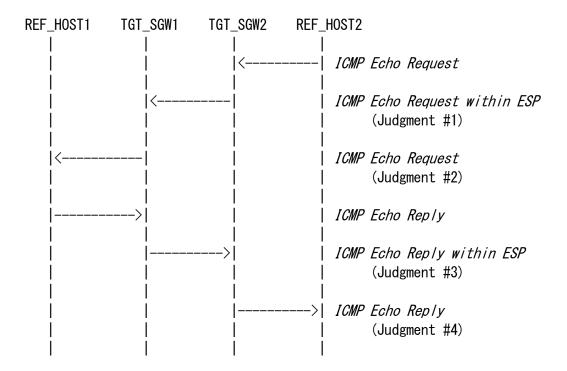
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.2.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node: N/A

SGW : ADVANCED (A requirement for all SGW NUTs that can select ICMP Type

as SPD selector, if you choose SGW vs. SGW Tunnel mode)

References:

- [RFC4301]

- [RFC4303]

- [RFC4443]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:

REF_HOST2 TGT_SGW2	- TGT_SGW1	- REF_HOST1	
SGW2_SA1-0>	SGW1_SA1-I	ICMPv6 Echo	Request
SGW2_SA1-I <	SGW1_SA1-0	ICMPv6 Echo	Request
SGW2_SA2-0>	SGW1_SA2-I	ICMPv6 Echo	Reply
SGW2 SA2-I <	SGW1 SA2-0	ICMPv6 Echo	Reply



Security Association Database (SAD) for SGW1 SA1-I

,
TGT_SGW2_Link2
TGT_SGW1_Link1
0x1000
tunnel
ESP
3DES-CBC
ipv6readylogo3des2to1req
HMAC-SHA1
ipv6readysha12to1req

Security Policy Database (SPD) for $SGW1_SA1-I$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA1-0

· · · · · · · · · · · · · · · · · · ·	
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for SGW1_SA1-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2 SA1-I

51 Gan2_6/(1 1
TGT_SGW1_Link1
TGT_SGW2_Link2
0x2000
tunnel
ESP
3DES-CBC
ipv6readylogo3des1to2req
HMAC-SHA1
ipv6readysha11to2req

Security Policy Database (SPD) for SGW2_SA1-I

	_
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA1-0

()	Total 10 710 cool action basabace (ens) 101 canz_oni	
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3des2to1req	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha12to1req	

Security Policy Database (SPD) for $SGW2_SA1-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW1 SA2-I

1 3411_3/12 1
TGT_SGW2_Link2
TGT_SGW1_Link1
0x3000
tunnel
ESP
3DES-CBC
ipv6readylogo3des2to1rep
HMAC-SHA1
ipv6readysha12to1rep

Security Policy Database (SPD) for SGW1_SA2-I

	_
Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA2-0

	-
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for SGW1_SA2-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA2-I

(6/12	, 10. Ganz_GAZ :
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for SGW2_SA2-I

	_
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA2-0

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD) for SGW2_SA2-0

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request1 within ESP1

zem zeme megaeee		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1req
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request1

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply1

IP Header	Source Address	REF_H0ST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply1 within ESP1

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des1to2rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2rep
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



ICMP Echo Request2 within ESP2

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	128 (Echo Request)

ICMP Echo Request2

IP Header	Source Address	REF_H0ST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	128 (Echo Request)

ICMP Echo Reply2

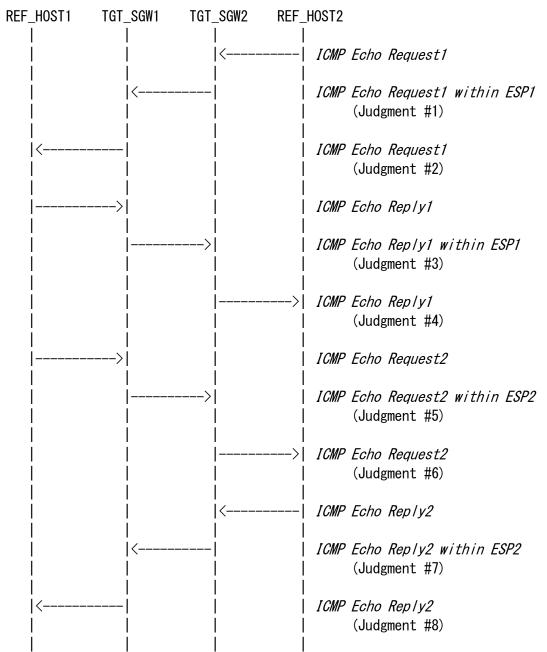
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply2 within ESP2

, ,		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Туре	129 (Echo Reply)



Procedure:





- 1. REF_HOST2 sends "ICMP Echo Request1" to REF_HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT SGW1 to TGT SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2
- 7. REF_HOST1 sends "ICMP Echo Request1" to REF_HOST2
- 8. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 9. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 10. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 11. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 12. Save the command log on REF_HOST1

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST1 and REF_HOST2.

Judgment:

```
Judgment #1
  Step-2: TGT_SGW2 transmits "ICMP Echo Request1 within ESP1"
Judgment #2
 Step-3: TGT_SGW1 transmits "ICMP Echo Request1"
Judgment #3
  Step-4: TGT_SGW1 transmits "ICMP Echo Reply1 within ESP1"
Judgment #4
  Step-5: TGT_SGW2 transmits "ICMP Echo Reply1"
Judgment #5
  Step-8: TGT_SGW1 transmits "ICMP Echo Request2 within ESP2"
Judgment #6
  Step-9: TGT SGW2 transmits "ICMP Echo Reguest2"
Judgment #7
  Step-10: TGT_SGW2 transmits "ICMP Echo Reply2 within ESP2"
Judgment #8
  Step-11: TGT_SGW1 transmits "ICMP Echo Reply2"
```

Possible Problems:

None.



5.2.9. Tunnel Mode: dummy packet handling

Purpose:

Verify that device can handle dummy packet as part of traffic flow confidentiality

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support dummy packet

handling if you choose SGW vs. SGW Tunnel mode)

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1 SA-I

Total 12) Modern Parabase (OND) 101 Cant_on 1	
TGT_SGW2_Link2	
TGT_SGW1_Link1	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbc2to1	
HMAC-SHA1	
ipv6readylogsha12to1	

Security Policy Database (SPD) for SGW1_SA-I

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

•	·
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

Total 10, 7,0000 action bacabase (one, 10, canz_on 1			
source address	TGT_SGW1_Link1		
destination address	TGT_SGW2_Link2		
SPI	0x2000		
mode	tunnel		
protocol	ESP		
ESP algorithm	3DES-CBC		
ESP key	ipv6readylogo3descbc1to2		
ESP authentication	HMAC-SHA1		
ESP authentication key	ipv6readylogsha11to2		

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



dummy packet 1

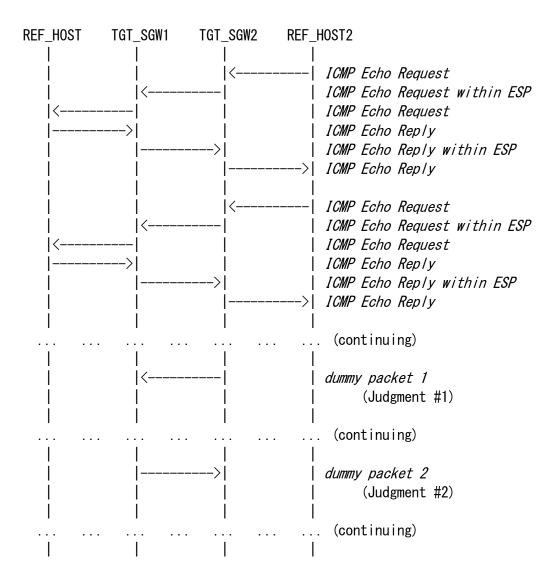
Source Address	TGT_SGW2_Link2
Destination Address	TGT_SGW1_Link1
SPI	0x1000
Algorithm	3DES-CBC
Key	ipv6readylogo3descbc2to1
Authentication Algorithm	HMAC-SHA1
Authentication Key	ipv6readylogsha12to1
Next Header	59 (no next header)
	Destination Address SPI Algorithm Key Authentication Algorithm Authentication Key

dummy packet 2

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	Next Header	59 (no next header)



Procedure:



- 1. REF_HOST2 keeps sending "ICMP Echo Request" to REF_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 4. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "dummy packet 1"

Judgment #3

Step-3: TGT_SGW1 transmits "dummy packet 2"

Possible Problems:

None.



5.2.10. Tunnel Mode: TFC padding

Pur	pose	٠
-----	------	---

Verify that device can handle TFC padding as part of traffic flow confidentiality

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support TFC padding

handling if you choose SGW vs. SGW Tunnel mode)

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

Total 1 to 7 to 5 to 1		
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for SGW1_SA-I

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

Total 1 by Model 1 at 1 but about 6 (c/lb) 1 c 1 cult 2 cm 2		
source address	TGT_SGW1_Link1	
destination address	TGT_SGW2_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for SGW2_SA-I

Tunnel source address	TGT_SGW1_Link1	
Tunnel destination address	TGT_SGW2_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for SGW2_SA-0

source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)



ICMP Echo Request within TFC padded ESP

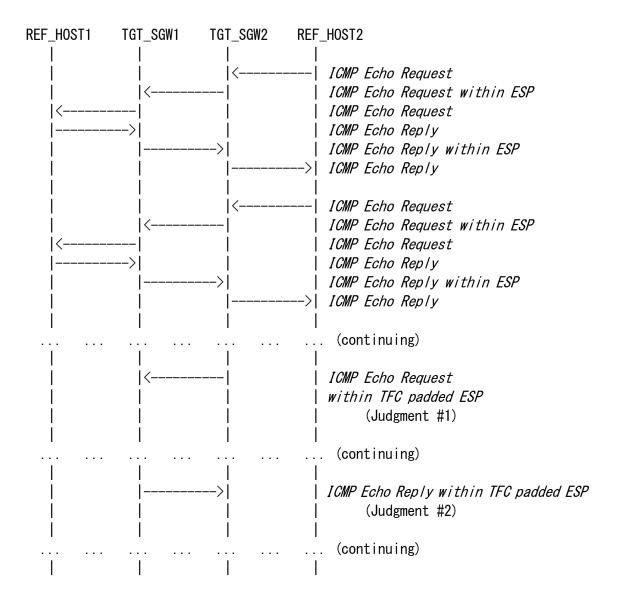
, ,		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within TFC padded ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	TFC padding	any size other than 0 byte
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 keeps sending "ICMP Echo Request" to REF_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 4. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within TFC padded ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Reply within TFC padded ESP"

Possible Problems:

None.



5.2.11. Tunnel Mode: Fragmentation

Purpose:

Verify that device can handle ICMPv6 Error Message (Packet Too Big) and packet fragmentation/reassembly.

Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs if you choose SGW vs. SGW Tunnel

mode)

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

Total 1 ty house at the bacasacs (one) for sair on 1		
source address	TGT_SGW2_Link2	
destination address	TGT_SGW1_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $SGW1_SA-I$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

Total ity house action bacasace (chb) for canz_on i		
source address	TGT_SGW1_Link1	
destination address	TGT_SGW2_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for SGW2_SA-I

T 1	TOT COMM I' I I
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

	_
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Error Message to REF_HOST2 (Packet Too Big)

		<u> </u>
IP Header	Source Address	TGT_SGW2
	Destination Address	REF_HOST2
ICMP	Туре	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Request

Fragmented ICMP Echo Request 1

IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

Fragmented ICMP Echo Request 2

Tragmented Tem Lene Negatet L		
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	REF_H0ST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request



Fragmented ICMP Echo Request within ESP 1

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

Fragmented ICMP Echo Request within ESP 2

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_H0ST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request

ICMP Echo Reply

I Chin Lond Hopiy		
IP Header	Source Address	REF_H0ST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Type	129 (Echo Reply)



ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
	Payload Length	1460
ICMP	Type	129 (Echo Reply)

ICMP Error Message to TGT_SGW1 (Packet Too Big)

IP Header	Source Address	REF_ROUTER1
	Destination Address	TGT_SGW1
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply
		within ESP

ICMP Error Message to REF_HOST1 (Packet Too Big)

IP Header	Source Address	TGT_SGW1
	Destination Address	REF_H0ST1_Link0
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply

Fragmented ICMP Echo Reply 1

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	129 (Echo Reply)



Fragmented ICMP Echo Reply 2

IP Header	Source Address	REF_H0ST1_Link0
	Destination Address	REF_H0ST2_Link3
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply

Fragmented ICMP Echo Reply within ESP 1

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	129 (Echo Reply)

Fragmented ICMP Echo Reply within ESP 2

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply



Procedure:

REF_HOST1	TGT_SGW1	REF_ROUTER1	TGT_	_SGW2 REF_	_HOST2
				 <	 ICMP Echo Request
				> 	 <i>ICMP Error Message to REF_HOST2</i> <i>(Packet Too Big)</i> (Judgment #1)
					 Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2
	 <	 	 		Fragmented ICMP Echo Request within ESP 1 Fragmented ICMP Echo Request within ESP 2 (Judgment #2)
 < <	 				 Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2 (Judgment #3)
	>				ICMP Echo Reply
	 	 	 > 		 <i>ICMP Echo Reply within ESP</i> (Judgment #4)
	 <	 			 ICMP Error Message to TGT_SGW1 (Packet Too Big)
					 Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2
	 <	 !	 		Fragmented ICMP Echo Request within ESP 1 Fragmented ICMP Echo Request within ESP 2 (Judgment #5)
 < <	 				 Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2 (Judgment #6)
	>				 ICMP Echo Reply
 < 	 				 <i>ICMP Error Message to REF_HOST1</i> <i>(Packet Too Big)</i> (Judgment #7)
I	 Cont	 inue to N ext P	age		



REF_HOST1	TGT_SGW1	REF_ROUTER1	TGT_SGW2	REF_HOST2
			 < <	 Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2
	 < 	 	 	Fragmented ICMP Echo Request within ESP 1 Fragmented ICMP Echo Request within ESP 2 (Judgment #8)
 < 	 			Fragmented ICMP Echo Request 1 Fragmented ICMP Echo Request 2 (Judgment #9)
 	> > 			Fragmented ICMP Echo Reply 1 Fragmented ICMP Echo Reply 2
	 	 	> > 	Fragmented ICMP Echo Reply within ESP 1 Fragmented ICMP Echo Reply within ESP 2 (Judgment #10)
				> Fragmented ICMP Echo Reply 1 > Fragmented ICMP Echo Reply 2 (Judgment #11)

- 1. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 3. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 5. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 6. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 7. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 8. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 9. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 10. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 11. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 12. Observe the packet transmitted from TGT SGW2 to TGT SGW1
- 13. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 14. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 15. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 16. Disconnect TGT_SGW1 and TGT_SGW2. Connect TGT_SGW2 to Link0. Connect TGT_SGW1 to Link1. Switch the roles of TGT_HOST1 and TGT_HOST2. Repeat step 1 to step 15

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Error Message to REF_HOST2 (Packet Too Big)" Judgment #2

Step-4: TGT_SGW2 transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

Judgment #3

Step-5: TGT_SGW1 transmits "Fragmented ICMP Echo Request 1" and "Fragmented ICMP Echo Request 2"

Judgment #4

Step-6: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #5

Step-8: TGT_SGW2 transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

Judgment #6

Step-9: TGT_SGW1 transmits "Fragmented ICMP Echo Request 1" and "Fragmented ICMP Echo Request 2"

Judgment #7

Step-10: TGT_SGW1 transmits "ICMP Error Message to REF_HOST1 (Packet Too Big)"
Judgment #8

Step-12: TGT_SGW2 transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

Judgment #9

Step-13: TGT_SGW1 transmits "Fragmented ICMP Echo Request 1" and "Fragmented ICMP Echo Request 2"

Judgment #10

Step-14: TGT_SGW1 transmits "Fragmented ICMP Echo Reply within ESP 1" and "Fragmented ICMP Echo Reply within ESP 2"

Judgment #11

Step-15: TGT_SGW2 transmits "Fragmented ICMP Echo Reply 1" and "Fragmented ICMP Echo Reply 2"

Possible Problems:

None.



5.2.12. Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256

Purpose:

Tunnel mode between two SGWs, ESP=3DES-CBC HMAC-SHA-256

Category:

End-Node : N/A

SGW : ADVANCED (A requirement for all SGW NUTs that support HMAC-SHA-256

as an authentication algorithm if you choose SGW vs. SGW Tunnel Mode)

References:

- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4868]

Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



Security Association Database (SAD) for SGW1_SA-I

,,,,,,,,,,,,,,,,,,,	· · · · · · · · - · · · · · · · · · · ·
source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha22562to1

Security Policy Database (SPD) for SGW1_SA-I

TGT_SGW2_Link2
TGT_SGW1_Link1
Link3
Link0
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

·	·
source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha22561to2

Security Policy Database (SPD) for SGW1_SA-0

Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW2_SA-I

order to the contraction bandward (crib) to canort .		
source address	TGT_SGW1_Link1	
destination address	TGT_SGW2_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA-256	
ESP authentication key	ipv6readylogoph2ipsecsha22561to2	

Security Policy Database (SPD) for SGW2_SA-I

	_
Tunnel source address	TGT_SGW1_Link1
Tunnel destination address	TGT_SGW2_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW2_SA-0

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha22562to1

Security Policy Database (SPD) for $SGW2_SA-0$

Tunnel source address	TGT_SGW2_Link2
Tunnel destination address	TGT_SGW1_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP

zem zeme megaeee		
IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha22562to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply

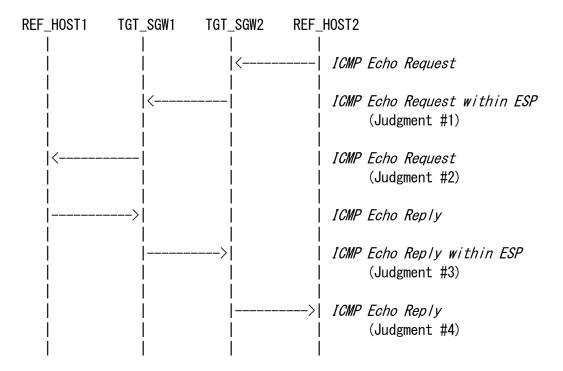
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
ICMP	Туре	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha22561to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF HOST2 sends "ICMP Echo Request" to REF HOST1
- 2. Observe the packet transmitted from TGT_SGW2 to TGT_SGW1
- 3. Observe the packet transmitted from TGT_SGW1 to REF_HOST1
- 4. Observe the packet transmitted from TGT_SGW1 to TGT_SGW2
- 5. Observe the packet transmitted from TGT_SGW2 to REF_HOST2
- 6. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT_SGW2 transmits "ICMP Echo Request within ESP"

Judgment #2

Step-3: TGT_SGW1 transmits "ICMP Echo Request"

Judgment #3

Step-4: TGT_SGW1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-5: TGT_SGW2 transmits "ICMP Echo Reply"

Possible Problems:

None.



5.3. Tunnel Mode (End-Node vs. SGW)

Scope:

Following tests focus on Tunnel Mode between End-Node and SGW.

Overview:

Tests in this section verify that a node properly processes and transmits the packets to which IPsec Tunnel Mode is applied between End-Node and SGWs.



5.3.1. Tunnel Mode: ESP=3DES-CBC HMAC-SHA1

Purpose:

Tunnel mode between End-Node and SGW, ESP=3DES-CBC HMAC-SHA1

Category:

End-Node: BASIC (A requirement for all End-Node NUTs if you choose End-Node vs.

SGW Tunnel Mode)

SGW : BASIC (A requirement for all SGW NUTs if you choose End-Node vs. SGW

Tunnel Mode)

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_H0ST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1 SA-I	<	SGW1 SA-O	



Security Association Database (SAD) for SGW1 SA-I

Total Tel Medical Bacabaco (GNB) Tot Gain _GN 1		
TGT_HOST1_Link0		
TGT_SGW1_Link1		
0x2000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcetos		
HMAC-SHA1		
ipv6readylogsha1etos		

Security Policy Database (SPD) for $SGW1_SA-I$

TGT_HOST1_Link0
TGT_SGW1_Link1
TGT_HOST1_Link0
REF_H0ST2_Link2
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

11.	TOT COM1 1 ' 11
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA-I

(one) 100 1 100 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcstoe	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1stoe	

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_H0ST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST1_SA-0

· · ·	·
source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_H0ST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

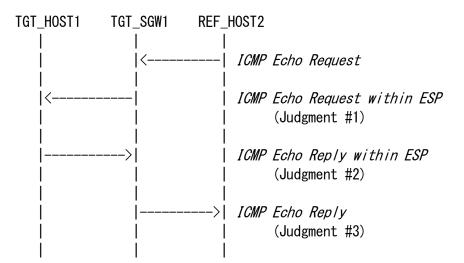
IP Header	Source Address	TGT_H0ST1_Link0
Destination Address		TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
I CMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel". Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.2. Tunnel Mode: ESP=3DES-CBC AES-XCBC

Purpose:

Tunnel mode between End-Node and SGW, ESP=3DES-CBC AES-XCBC

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC

as an authentication algorithm if you choose End-Node vs. SGW Tunnel

Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-XCBC as an

authentication algorithm if you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1 REF_HOST2
HOST1_SA-0	>	SGW1_SA-I
HOST1_SA-I	<	SGW1_SA-O



Security Association Database (SAD) for SGW1_SA-I

Total 1 by Modern Bacasace (ons) 101 can _on _		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcetos	
ESP authentication	AES-XCBC	
ESP authentication key	ipv6readaesxetos	

Security Policy Database (SPD) for SGW1_SA-I

TGT_HOST1_Link0
TGT_SGW1_Link1
TGT_HOST1_Link0
REF_H0ST2_Link2
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

•	•
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesxstoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	0ut
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA-I

(0/15) /10000 / 401011 Buttabass (0/15) / 101 1100 / 1_0/1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcstoe	
ESP authentication	AES-XCBC	
ESP authentication key ipv6readaesxstoe		

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_H0ST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	AES-XCBC
ESP authentication key ipv6readaesxetos	

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
Destination Address		TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesxetos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

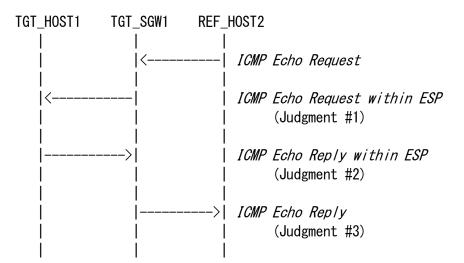
IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesxstoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel".

Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.3. Tunnel Mode: ESP=3DES-CBC NULL

Purpose	:
-	

Tunnel mode between End-Node and SGW, ESP=3DES-CBC NULL

Removed at revision 1.11.0.



5.3.4. Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between End-Node and SGW, ESP-AES-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

AES-CBC(128-bit) as an encryption algorithm if you choose End-Node

vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CBC (128-bit)

as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC2404]

- [RFC2451]

- [RFC3602]

- [RFC4301]

- [RFC4303]

- [RFC4305]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_HOST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1_SA-I	<	SGW1_SA-0	



Security Association Database (SAD) for SGW1 SA-I

Total 125 Moderation Business (OND) 101 Guill_ON 1	
TGT_HOST1_Link0	
TGT_SGW1_Link1	
0x2000	
tunnel	
ESP	
AES-CBC(128-bit)	
ipv6readaescetos	
HMAC-SHA1	
ipv6readylogsha1etos	

Security Policy Database (SPD) for $SGW1_SA-I$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

_SGW1_Link1
_HOST1_LinkO
000
ne l
-CBC(128-bit)
Greadaescstoe
C-SHA1
Greadylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_LinkO
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1 SA-I

Total Tel Medical Bacabaco (GNB) Tot Medit_GN 1	
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC (128-bit)
ESP algorithm key	ipv6readaescstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

occurred Acceptance (eng., for mostillizer, c		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CBC(128-bit)	
ESP algorithm key	ipv6readaescetos	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

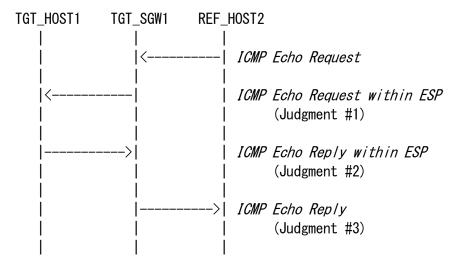
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	AES-CBC (128-bit)
	Key	ipv6readaescstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel".

Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.5. Tunnel Mode: ESP=AES-CTR HMAC-SHA1

Purpose:

Tunnel mode between End-Node and SGW, ESP=AES-CTR HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-CTR

as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CTR as an

encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_H0ST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1_SA-I	<	SGW1_SA-0	



Security Association Database (SAD) for SGW1 SA-I

Total Tey Moderation Buttabase (ONB) Tot Sum_on I		
TGT_HOST1_Link0		
TGT_SGW1_Link1		
0x2000		
tunnel		
ESP		
AES-CTR		
ipv6readylogoaesetos		
HMAC-SHA1		
ipv6readylogsha1etos		

Security Policy Database (SPD) for $SGW1_SA-I$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

·
TGT_SGW1_Link1
TGT_HOST1_Link0
0x1000
tunnel
ESP
AES-CTR
ipv6readylogoaesstoe
HMAC-SHA1
ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_LinkO
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1 SA-I

Total 123 Moderation Bacasage (one) for modifical 1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP algorithm key	ipv6readylogoaesstoe	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1stoe	

Security Policy Database (SPD) for HOST1_SA-I

	_
tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

country, herocotation baseauce (chb) for heart _cht c		
source address	TGT_HOST1_LinkO	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP algorithm key	ipv6readylogoaesetos	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_LinkO
tunnel destination address	TGT_SGW1_Link1
source address	TGT_H0ST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogoaesetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

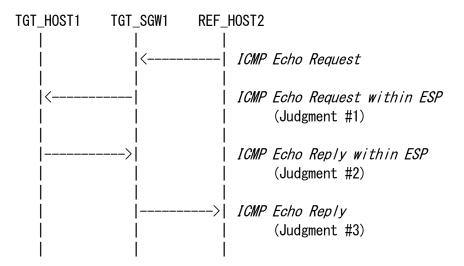
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogoaesstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel". Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

Tunnel mode between End-Node and SGW, ESP=NULL HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support NULL as

an encryption algorithm are required to satisfy if you choose

End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an

encryption algorithm are required to satisfy if you choose End-Node

vs. SGW Tunnel Mode)

References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1 REF_HOST2
HOST1_SA-0	>	SGW1_SA-I
HOST1 SA-I	<	SGW1 SA-0



Security Association Database (SAD) for SGW1_SA-I

Total 1 ty Modern Paragraph (ONE) 101 Call 1_ON 1		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP algorithm key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for SGW1_SA-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

·	—
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP algorithm key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1 SA-I

Total Tel Medical Bacabaco (GNB) Tot Medit_GN 1		
TGT_SGW1_Link1		
TGT_HOST1_Link0		
0x1000		
tunnel		
ESP		
NULL		
HMAC-SHA1		
ipv6readylogsha1stoe		

Security Policy Database (SPD) for HOST1_SA-I

	_
tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP algorithm key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_LinkO
tunnel destination address	TGT_SGW1_Link1
source address	TGT_H0ST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

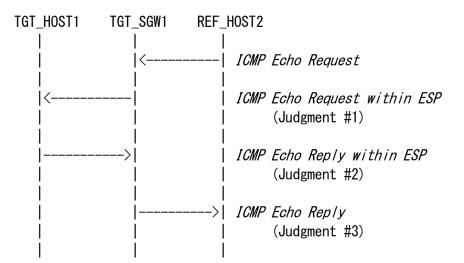
IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
I CMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel".

Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.7. Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between End-Node and SGW, ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose

End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support

CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose

End-Node vs. SGW Tunnel Mode)

References:

- [RFC2404]

- [RFC2451]

- [RFC4301]

- [RFC4303]

- [RFC4305]

- [RFC4312]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1 REF_HOST2
HOST1_SA-0	>	SGW1_SA-I
HOST1 SA-I	<	SGW1 SA-0



Security Association Database (SAD) for SGW1_SA-I

source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP algorithm key	ipv6readcamcetos	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for SGW1_SA-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	Any
direction	In
protocol	ESP
mode	Tunnel

Security Association Database (SAD) for SGW1_SA-0

·	—
source address	TGT_SGW1_Link1
destination address	TGT_H0ST1_Link0
SPI	0x1000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Security Association Database (SAD) for HOST1_SA-I

Total 1 to The total business (only 1 or 11 or 1 _ or 1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_LinkO	
SPI	0x1000	
mode	Tunnel	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP algorithm key	ipv6readcamcstoe	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1stoe	

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_H0ST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	Any	
direction	In	
protocol	ESP	
mode	Tunnel	

Security Association Database (SAD) for HOST1_SA-0

codd, rej moderation bacasace (one) for modificant		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	Tunnel	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP algorithm key	ipv6readcamcetos	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

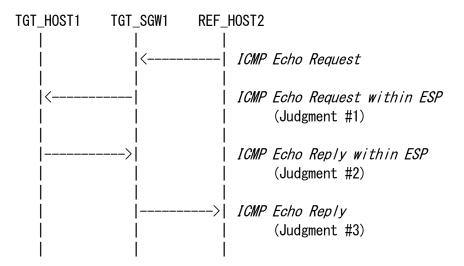
IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel". Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.3.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that can select ICMP

Type as SPD selector if you choose End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that can select ICMP Type

as SPD selector if you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC4301]
- [RFC4303]
- [RFC4443]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_HOST2		
HOST1_SA1-0	>	SGW1_SA1-I	ICMPv6	Echo	Request
HOST1_SA1-I	<	SGW1_SA1-0	ICMPv6	Echo	Request
HOST1_SA2-0	>	SGW1_SA2-I	ICMPv6	Echo	Reply
HOST1_SA2-I	<	SGW1_SA2-0	ICMPv6	Echo	Reply



Security Association Database (SAD) for SGW1 SA1-I

Total 12 Mode of a cross parabases (only 101 can 1_only 1		
TGT_HOST1_Link0		
TGT_SGW1_Link1		
0x2000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3desetosreq		
HMAC-SHA1		
ipv6readysha1etosreq		

Security Policy Database (SPD) for $SGW1_SA1-I$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $SGW1_SA1-0$

·	—
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3desstoereq
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1stoereq

Security Policy Database (SPD) for SGW1_SA1-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_LinkO
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA1-I

Total 10) Notice and Database (only 10) Not 1_011 1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3desstoereq	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha1stoereq	

Security Policy Database (SPD) for HOST1_SA1-I

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA1-0

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3desetosreq
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1etosreq

Security Policy Database (SPD) for HOST1_SA1-0

tunnel source address	TGT_H0ST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for SGW1_SA2-I

100001 10) 1100001 40101 Bacasaco (6/15) 101 04111_0/12 1		
source address	TGT_HOST1_LinkO	
destination address	TGT_SGW1_Link1	
SPI	0x4000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3desetosrep	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha1etosrep	

Security Policy Database (SPD) for SGW1_SA2-I

	<u> </u>
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA2-0

	
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3desstoerep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1stoerep

Security Policy Database (SPD) for SGW1_SA2-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA2-I

source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x3000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3desstoerep	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha1stoerep	

Security Policy Database (SPD) for HOST1_SA2-I

TGT_SGW1_Link1
TGT_HOST1_Link0
REF_H0ST2_Link2
TGT_HOST1_Link0
ICMPv6 Echo Reply
in
ESP
tunnel

Security Association Database (SAD) for HOST1_SA2-0

2004110) /10001401011 Butuabus (0/15) 101 110011_0/12 0		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x4000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3desetosrep	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha1etosrep	

Security Policy Database (SPD) for HOST1_SA2-0

tunnel source address	TGT_H0ST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request1

IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request1 within ESP1 tunnel

	. III ciiiii Loi i caiiiioi	
IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desstoereq
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1stoereq
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply1 within ESP1 tunnel

, ,		
IP Header	Source Address	TGT_HOST1_LinkO
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desetosrep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosrep
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply1

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



ICMP Echo Request2 within ESP2 tunnel

Zom Lone noque	OLL WILLIAM LOIL COMMING	
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desetosreq
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosreq
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Туре	128 (Echo Request)

ICMP Echo Request2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	128 (Echo Request)

ICMP Echo Reply2

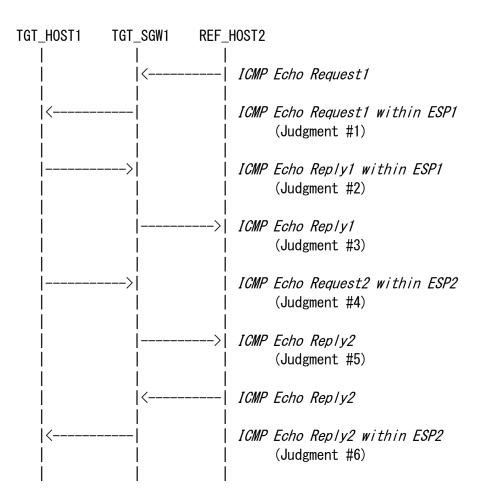
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply2 within ESP2 tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desstoerep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1stoerep
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request1" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2
- 6. TGT HOST1 sends "ICMP Echo Request2 within ESP2" to REF HOST2
- 7. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 8. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 9. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 10. Save the command log on TGT_HOST1

NOTE: REF_HOST2 must have an ability to send ICMP Echo Request



Judgment:

```
Judgment #1
Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request1 within ESP1 tunnel".

Judgment #2
Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply1 within ESP1 tunnel".

Judgment #3
Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply1".

Judgment #4
Step-7: TGT-HOST1 transmits the packet "ICMP Echo Request2 within ESP2 tunnel".

Judgment #5
Step-8: TGT-SGW1 transmits the packet "ICMP Echo Request2".

Judgment #6
Step-9: TGT-SGW1 transmits the packet "ICMP Echo Reply within ESP2 tunnel".
```

Possible Problems:

TGT_HOST1 may be a passive node which does not implement an application for sending Echo Requests. The another method to perform this test is required for the passive node. (see Appendix-C)



5.3.9. Tunnel Mode: dummy packet handling

Purpose:

Verify that device can handle dummy packet as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support dummy packet

handling if you choose End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support dummy packet

handling if you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_HOST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1 SA-I	<	SGW1 SA-0	



Security Association Database (SAD) for SGW1_SA-I

• • • • • • • • • • • • • • • • • • • •	—
source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for SGW1_SA-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $SGW1_SA-0$

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	0ut
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA-I

(one) 100 1 100 100 100 100 100 100 11 100 1		
source address	TGT_SGW1_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcstoe	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1stoe	

Security Policy Database (SPD) for HOST1_SA-I

	_
tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

	TOT HOOTE I' LO
source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

Zem Zene nepry mremm zen zemmen			
IP Header Source Address		TGT_HOST1_Link0	
	Destination Address	TGT_SGW_Link1	
ESP SPI 0x20		0x2000	
	Algorithm	3DES-CBC	
Key Authentication Algorithm		ipv6readylogo3descbcstoe	
		HMAC-SHA1	
	Authentication Key	ipv6readylogsha1stoe	
IP Header	Source Address	TGT_HOST1_Link0	
	Destination Address	REF_HOST2_Link2	
ICMP	Type	129 (Echo Reply)	

ICMP Echo Reply

IP Header	Source Address TGT_HOST1_Link0	
	Destination Address	REF_H0ST2_Link2
I CMP	Type	129 (Echo Reply)



dummy packet 1

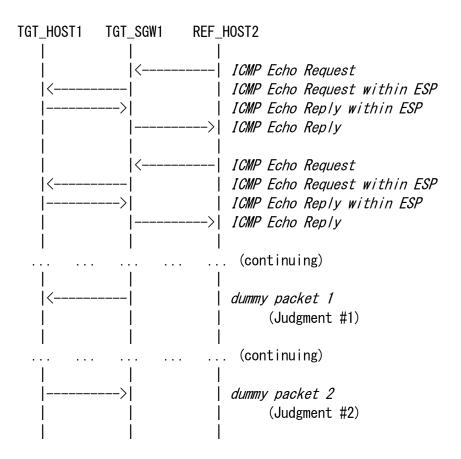
IP Header Source Address		TGT_SGW_Link1
	Destination Address	TGT_HOST1_LinkO
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
Authentication Algorithm HMAG		HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
	Next Header	59 (no next header)

dummy packet 2

IP Header Source Address		TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP SPI		0x2000
	Algorithm	3DES-CBC
		ipv6readylogo3descbcstoe
		HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
	Next Header	59 (no next header)



Procedure:



- 1. REF_HOST2 keeps sending "ICMP Echo Request" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "dummy packet 1".

Judgment #2

Step-3: TGT-HOST1 transmits the packet "dummy packet 2".

Possible Problems:

None.



5.3.10. Tunnel Mode: TFC padding

Purpose:

Verify that device can handle TFC padding as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support TFC padding

if you choose End-Node vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support TFC padding if

you choose End-Node vs. SGW Tunnel Mode)

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_HOST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1 SA-I	<	SGW1 SA-0	



Security Association Database (SAD) for SGW1 SA-I

Total 1 to 1 t		
TGT_HOST1_Link0		
TGT_SGW1_Link1		
0x2000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcetos		
HMAC-SHA1		
ipv6readylogsha1etos		

Security Policy Database (SPD) for $SGW1_SA-I$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

·	=
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	0ut
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA-I

Country Mesocration Passaces (CMS) for Mosti_CM I		
TGT_SGW1_Link1		
TGT_H0ST1_Link0		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcstoe		
HMAC-SHA1		
ipv6readylogsha1stoe		

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_H0ST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

Temm Terre riepry mremmer		
IP Header	Source Address	TGT_HOST1_LinkO
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
I CMP	Type	129 (Echo Reply)



ICMP Echo Request within TFC padded ESP tunnel

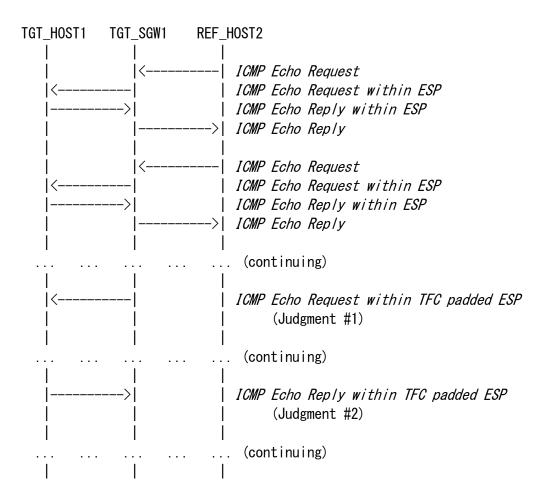
IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
	TFC padding	any size other than 0 byte
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
	TFC padding	any size other than 0 byte
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 keeps sending "ICMP Echo Request" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.



Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within TFC padded ESP tunnel".

Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within TFC padded ESP tunnel".

Possible Problems:

None.



5.3.11. Tunnel Mode: Fragmentation

Purpose:

Verify that device can handle ICMPv6 Error Message (Packet Too Big) and packet fragmentation/reassembly.

Category:

End-Node: BASIC (A requirement for all End-Node NUTs if you choose End-Node vs.

SGW Tunnel Mode)

SGW : BASIC (A requirement for all SGW NUTs if you choose End-Node vs. SGW

Tunnel Mode)

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

Initialization (Parts A and B):

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1	REF_H0ST2
HOST1_SA-0	>	SGW1_SA-I	
HOST1_SA-I	<	SGW1_SA-O	



Security Association Database (SAD) for SGW1 SA-I

Total 1 ty Mode of a trial battabase (only for ball 1_on 1		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcetos	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1etos	

Security Policy Database (SPD) for $SGW1_SA-I$

TGT_HOST1_Link0
TGT_SGW1_Link1
TGT_HOST1_Link0
Link2 + Link3
any
in
ESP
tunnel

Security Association Database (SAD) for SGW1_SA-0

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	Link2 + Link3
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1 SA-I

Total Tey Mode Tat Total Batabase (SMB) Tot Mod T_SM 1		
TGT_SGW1_Link1		
TGT_HOST1_Link0		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcstoe		
HMAC-SHA1		
ipv6readylogsha1stoe		

Security Policy Database (SPD) for HOST1_SA-I

	_
tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	Link2 + Link3
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

` \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	TOT HOOT1 I' LO
source address	TGT_HOST1_LinkO
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	Link2 + Link3
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets (Part A):

Fragmented ICMP Echo Request 1

	-	
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Туре	128 (Echo Request)

Fragmented ICMP Echo Request 2

Tragmorted Tom Lorio Reducet L		
IP Header	Source Address	REF_H0ST2_Link3
	Destination Address	TGT_HOST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request

Fragmented ICMP Echo Request 1 within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Туре	128 (Echo Request)



Fragmented ICMP Echo Request 2 within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	TGT_HOST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
	Payload Length	1460
ICMP	Type	129 (Echo Reply)

ICMP Error Message to TGT_HOST1 (Packet Too Big)

IP Header	Source Address	REF_ROUTER2
	Destination Address	TGT_HOST1
ICMP	Туре	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply



Fragmented ICMP Echo Reply 1 within ESP

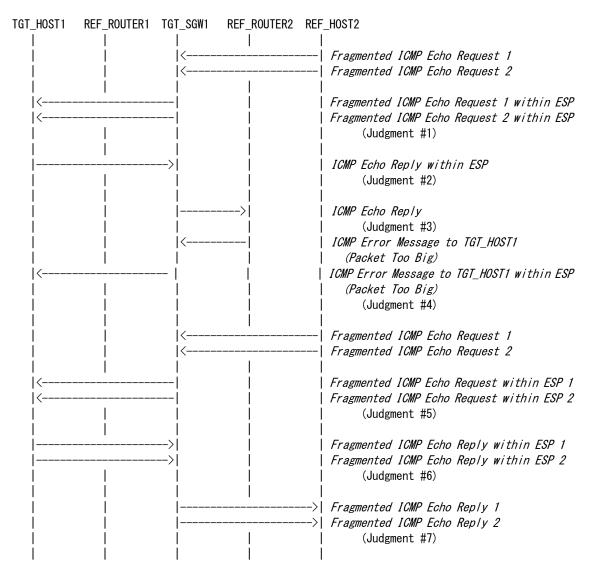
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link3
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Туре	129 (Echo Reply)

Fragmented ICMP Echo Reply 2 within ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link3
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply



Procedure (Part A):



- 1. Configure Link3 with an MTU of 1280 Bytes. All other Links are set to the default MTU.
- 2. REF_HOST2 sends a "ICMP Echo Request" to REF_HOST1
- 3. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 4. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 5. Observe the packet transmitted from TGT_SGW11 to REF_ROUTER2
- 6. Observe the packet transmitted from TGT_SGW11 to TGT_HOST1
- 7. REF_HOST2 sends a "ICMP Echo Request" to REF_HOST1
- 8. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 9. Observe the packet transmitted from TGT HOST1 to TGT SGW1
- 10. Observe the packet transmitted from TGT_SGW1 to REF_HOST2



NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment (Part A):

Judgment #1

Step-3: TGT_SGW1 transmits "Fragmented ICMP Echo Request 1 within ESP" and "Fragmented ICMP Echo Request 2 within ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply within ESP"

Judgment #3

Step-5: TGT_HOST1 transmits "ICMP Echo Reply"

Judgment #4

Step-6: TGT_SGW1 transmits "ICMP Error Message to TGT_HOST1 (Packet Too Big) within ESP"

Judgment #5

Step-8: TGT_SGW1 transmits "Fragmented ICMP Echo Request 1 within ESP" and "Fragmented ICMP Echo Request 2 within ESP"

Judgment #6

Step-9: TGT_SGW1 transmits "Fragmented ICMP Echo Reply 1 within ESP" and "Fragmented ICMP Echo Reply 2 within ESP"

Judgment #7

Step-10: TGT_SGW1 transmits "Fragmented ICMP Echo Reply 1" and "Fragmented ICMP Echo Reply 2"

Possible Problems (Part A):

• The link technology on Link 1 may require fragmentation of the packet "Fragmented ICMP Echo Request within ESP 1". In this case, TGT_SGW1 may further fragment this packet.



Packets (Part B):

ICMP Echo Request

IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Error Message to REF_HOST2 (Packet Too Big)

		- ·
IP Header	Source Address	TGT_SGW1
	Destination Address	REF_HOST2
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Request

Fragmented ICMP Echo Request 1

IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Туре	128 (Echo Request)

Fragmented ICMP Echo Request 2

Tragmenteda 10mm 20	Tragmerreda Iem Zerre Negace Z		
IP Header	Source Address	REF_H0ST2_Link2	
	Destination Address	TGT_HOST1_Link0	
	Payload Length	2ndPL (= 1476-1stPL)	
Fragment	Offset	(1stPL-8)/8	
	More Flag	0	
Data	Data	Rest of ICMP Echo Request	



Fragmented ICMP Echo Request within ESP 1

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_H0ST2_Link2
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

Fragmented ICMP Echo Request within ESP 2

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request



ICMP Echo Reply within ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
	Payload Length	1460
ICMP	Туре	129 (Echo Reply)

ICMP Error Message to TGT_HOST1 (Packet Too Big)

IP Header	Source Address	REF_ROUTER1
	Destination Address	TGT_HOST1
ICMP	Туре	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply
		within ESP



Fragmented ICMP Echo Reply within ESP 1

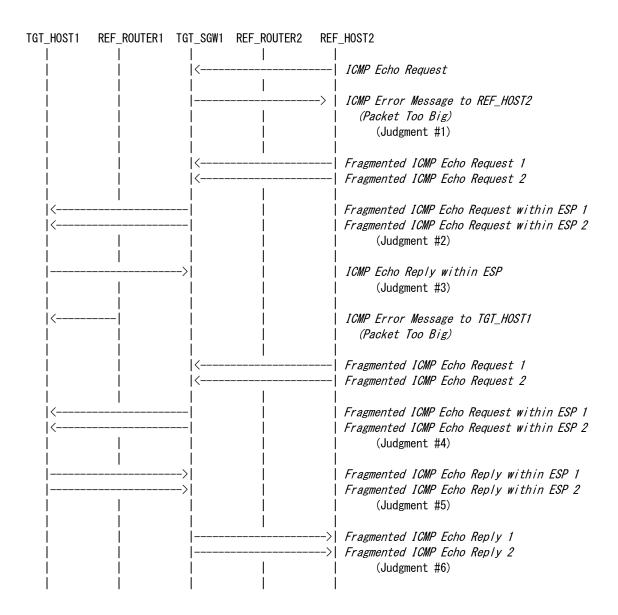
IP Header Source Address		TGT_HOST1_Link0
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
Authentication Key		ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	129 (Echo Reply)

Fragmented ICMP Echo Reply within ESP 2

IP Header Source Address Destination Address		TGT_HOST1_Link0
		TGT_SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
Authentication Key		ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply



Procedure (Part B):



- 1. Configure Link1 with an MTU of 1280 Bytes. All other Links are set to the default MTU.
- 2. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 3. Observe the packet transmitted from TGT SGW1 to REF HOST2
- 4. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 5. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 6. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 7. REF_HOST2 sends "ICMP Echo Request" to REF_HOST1
- 8. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 9. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1



10. Observe the packet transmitted from TGT_SGW1 to REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment (Part B):

Judgment #1

Step-3: TGT_SGW1 transmits "ICMP Error Message to REF_HOST2 (Packet Too Big)"
Judgment #2

Step-5: TGT_SGW1 transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

Judgment #3

Step-6: TGT_HOST1 transmits "ICMP Echo Reply within ESP"

Judgment #4

Step-8: TGT_SGW1 transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

Judgment #5

Step-9: TGT_HOST1 transmits "Fragmented ICMP Echo Reply within ESP 1" and "Fragmented ICMP Echo Reply within ESP 2"

Judgment #6

Step-10: TGT_SGW1 transmits "Fragmented ICMP Echo Reply 1" and "Fragmented ICMP Echo Reply 2"

Possible Problems (Part B):

When transmitting the packet "Fragmented ICMP Echo Request within ESP 1",
or "Fragmented ICMP Echo Reply within ESP 1", TGT_SGW1 or TGT_HOST1
further fragmentation may be required, depending on implementation choice.
In this case, these devices may choose to transmit data as either 2 or 3
fragments.



5.3.12. Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256

Purpose:

Tunnel mode between End-Node and SGW, ESP=3DES-CBC HMAC-SHA-256

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

HMAC-SHA-256 as an authentication algorithm if you choose End-Node

vs. SGW Tunnel Mode)

SGW : ADVANCED (A requirement for all SGW NUTs that support HMAC-SHA-256

as an authentication algorithm if you choose End-Node vs. SGW Tunnel

Mode)

References:

- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4868]

Initialization:

Use common topology described as Fig. 3 Set NUT's SAD and SPD as following:

TGT_HOST1		TGT_SGW1 REF_HOST2
HOST1_SA-0	>	SGW1_SA-I
HOST1 SA-I	<	SGW1 SA-0



Security Association Database (SAD) for SGW1_SA-I

Total 1 to 7 total at 1 to 1 bacasaco (crib) 1 or can 1_cri		
source address	TGT_HOST1_Link0	
destination address	TGT_SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcetos	
ESP authentication	HMAC-SHA-256	
ESP authentication key	ipv6readylogoph2ipsecsha2256etos	

Security Policy Database (SPD) for SGW1_SA-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_LinkO
destination address	REF_H0ST2_Link2
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA-0

	=
source address	TGT_SGW1_Link1
destination address	TGT_H0ST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha2256stoe

Security Policy Database (SPD) for SGW1_SA-0

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_H0ST2_Link2
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA-I

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha2256stoe

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_H0ST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST1_SA-0

source address	TGT_HOST1_LinkO
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcetos
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha2256etos

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_H0ST2_Link2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha2256etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

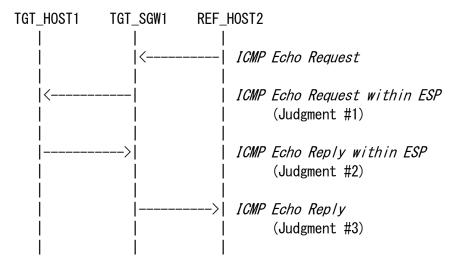
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha2256stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_H0ST2_Link2
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. REF_HOST2 sends "ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted from TGT_SGW1 to TGT_HOST1
- 3. Observe the packet transmitted from TGT_HOST1 to TGT_SGW1
- 4. Observe the packet transmitted from TGT_SGW1 to REF_HOST2
- 5. Save the command log on REF_HOST2

NOTE: Please choose a device which can send ICMP Echo Request as REF_HOST2.

Judgment:

Judgment #1

Step-2: TGT-SGW1 transmits the packet "ICMP Echo Request within ESP tunnel". Judgment #2

Step-3: TGT-HOST1 transmits the packet "ICMP Echo Reply within ESP tunnel". Judgment #3

Step-4: TGT-SGW1 transmits the packet "ICMP Echo Reply".

Possible Problems:

None.



5.4. Tunnel Mode (End-Node vs. End-Node)

Caana	
Scope	•

Following tests focus on Tunnel Mode between End-Node and End-Node.

Overview:

Tests in this section verify that a node properly processes and transmits the packets to which IPsec Tunnel Mode is applied between two End-Nodes.



5.4.1. Tunnel Mode: ESP=3DES-CBC HMAC-SHA1

Purpose:

Tunnel mode between two End-Nodes, ESP=3DES-CBC HMAC-SHA1

Category:

End-Node: BASIC (A requirement for all End-Node NUTs if you choose End-Node vs.

End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2]	rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1 SA-I

coodine y necochaeron paeasaco (ons) non necon_on i		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_HOST2_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for $HOST1_SA-0$

	-
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

· · · · · · · · · · · · · · · · · · ·	. =
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

tunnel source address	TGT_HOST1_Link0	
tunnel destination address	TGT_HOST2_Link1	
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST2_SA-0

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

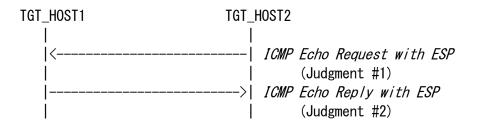
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.2. Tunnel Mode: ESP=3DES-CBC AES-XCBC

Purpose:

Tunnel mode between two End-Nodes, ESP=3DES-CBC AES-XCBC

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC

as an authentication algorithm if you choose End-Node vs. End-Node

Tunnel Mode)

: N/A SGW

References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1 SA-I

occurry hococration bacasaco (ons) for hoch i_on i		
TGT_HOST2_Link1		
TGT_HOST1_Link0		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbc2to1		
AES-XCBC		
ipv6readaesx2to1		

Security Policy Database (SPD) for $HOST1_SA-I$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $HOST1_SA-O$

•	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

Total 10) Moderna Parada acc (only 101 Modil_on 1	
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for HOST2_SA-I

	_
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA-0

	<u> </u>
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

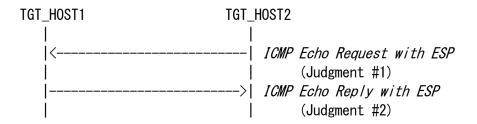
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx2to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx1to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.3. Tunnel Mode: ESP=3DES-CBC NULL

Pur	pose	٠
-----	------	---

Tunnel mode between two End-Nodes, ESP=3DES-CBC NULL

Removed at revision 1.11.0.



5.4.4. Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between two End-Nodes, ESP=AES-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

AES-CBC(128-bit) as an encryption algorithm if you choose End-Node

vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC2404]
- [RFC2451]
- [RFC3602]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	SA-0



Security Association Database (SAD) for HOST1_SA-I

total rej meeteration bacasace (ens) rei meeti_en :		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CBC (128-bit)	
ESP algorithm key	ipv6readaesc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST1_SA-I$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $HOST1_SA-O$

·	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

70000 100 70000 100 100 100 100 100 12_0/1 1	
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaesc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

tunnel source address	TGT_HOST1_Link0	
tunnel destination address	TGT_HOST2_Link1	
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for HOST2_SA-0

Total 10, 7,0000 action business (ens.) 101 monte_on o		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CBC(128-bit)	
ESP algorithm key	ipv6readaesc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

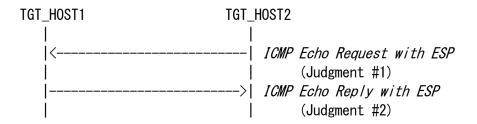
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaesc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CBC (128-bit)
	Key	ipv6readaesc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.5. Tunnel Mode: ESP=AES-CTR HMAC-SHA1

Purpose:

Tunnel mode between two End-Nodes, ESP=AES-CTR HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support AES-CTR

as an encryption algorithm if you choose End-Node vs. End-Node Tunnel

Mode)

: N/A SGW

References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	_SA-0



Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1		
destination address	TGT_HOST1_Link0		
SPI	0x1000		
mode	tunnel		
protocol	ESP		
ESP algorithm	AES-CTR		
ESP algorithm key	ipv6readylogoaes2to1		
ESP authentication	HMAC-SHA1		
ESP authentication key	ipv6readylogsha12to1		

Security Policy Database (SPD) for $HOST1_SA-I$

TGT_HOST2_Link1
TGT_HOST1_Link0
TGT_HOST2_Link1
TGT_HOST1_Link0
any
in
ESP
tunnel

Security Association Database (SAD) for $HOST1_SA-0$

•	=
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaes1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

Total 13 Modes (and based (and) 101 Modes 2011		
source address	TGT_HOST1_LinkO	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP algorithm key	ipv6readylogoaes1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for HOST2_SA-I

tunnel source address	TGT_HOST1_Link0		
tunnel destination address	TGT_HOST2_Link1		
source address	TGT_HOST1_Link0		
destination address	TGT_HOST2_Link1		
upper spec	any		
direction	in		
protocol	ESP		
mode	tunnel		

Security Association Database (SAD) for HOST2_SA-0

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CTR	
ESP algorithm key	ipv6readylogoaes2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key ipv6readylogsha12to1		

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

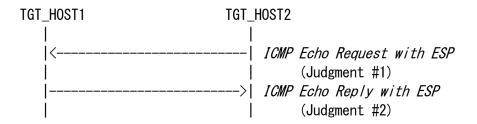
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

Tunnel mode between two End-Nodes, ESP=NULL HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support NULL as

an encryption algorithm if you choose End-Node vs. End-Node Tunnel

Mode)

: N/A SGW

References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2 SA-I	<	HOST1	SA-0



Security Association Database (SAD) for HOST1_SA-I

Total 125 Moode action Bacasace (ONE) 101 Mootingon 1		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_LinkO	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP algorithm key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST1_SA-I$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $HOST1_SA-0$

•	_
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP algorithm key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2 SA-I

Total Tey Moderation Batabase (OND) For Modifical I		
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP algorithm key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for HOST2_SA-I

TGT_HOST1_Link0		
TGT_HOST2_Link1		
TGT_HOST1_Link0		
TGT_HOST2_Link1		
any		
in		
ESP		
tunnel		

Security Association Database (SAD) for HOST2_SA-0

(one) 100 100 100 100 100 100 100 100 100 10		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP algorithm key		
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

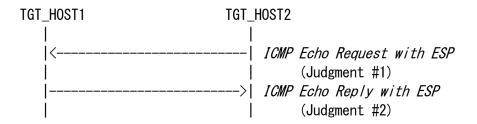
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.7. Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Purpose:

Tunnel mode between two End-Nodes, ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose

End-Node vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC2404]

- [RFC2451]

- [RFC4301]

- [RFC4303]

- [RFC4305]

- [RFC4312]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		rgt_hos	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	_SA-0



Security Association Database (SAD) for HOST1 SA-I

Cocarrey hoseoracron bacabase (onb) for hoser_on 1				
source address	TGT_HOST2_Link1			
destination address	TGT_HOST1_Link0			
SPI	0x1000			
mode	tunnel			
protocol	ESP			
ESP algorithm	CAMELLIA-CBC(128-bit)			
ESP algorithm key	ipv6readcamc2to1			
ESP authentication	HMAC-SHA1			
ESP authentication key	ipv6readylogsha12to1			

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_HOST2_Link1			
tunnel destination address	TGT_HOST1_Link0			
source address	TGT_HOST2_Link1			
destination address	TGT_HOST1_Link0			
upper spec	Any			
direction	In			
protocol	ESP			
mode	Tunnel			

Security Association Database (SAD) for $HOST1_SA-O$

· · · · · · · · · · · · · · · · · · ·	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Security Association Database (SAD) for HOST2_SA-I

Total 10) Noodo la di la dadada (one) 101 Noole_on 1				
source address	TGT_H0ST1_Link0			
destination address	TGT_H0ST2_Link1			
SPI	0x2000			
mode	Tunnel			
protocol	ESP			
ESP algorithm	CAMELLIA-CBC(128-bit)			
ESP algorithm key	ipv6readcamc1to2			
ESP authentication	HMAC-SHA1			
ESP authentication key	ipv6readylogsha11to2			

Security Policy Database (SPD) for HOST2_SA-I

2004110J 10110J 24042400 (012) 101 110012_0/1				
TGT_HOST1_Link0				
TGT_HOST2_Link1				
TGT_HOST1_Link0				
TGT_HOST2_Link1				
Any				
In				
ESP				
Tunnel				

Security Association Database (SAD) for HOST2_SA-0

Total 1 ty 710000 1 de la casació (chis) 101 110012_chi c				
source address	TGT_HOST2_Link1			
destination address	TGT_HOST1_Link0			
SPI	0x1000			
mode	Tunne I			
protocol	ESP			
ESP algorithm	CAMELLIA-CBC(128-bit)			
ESP algorithm key	ipv6readcamc2to1			
ESP authentication	HMAC-SHA1			
ESP authentication key	ipv6readylogsha12to1			

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_LinkO
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	Any
direction	Out
protocol	ESP
mode	Tunnel



Packets:

ICMP Echo Request within ESP tunnel

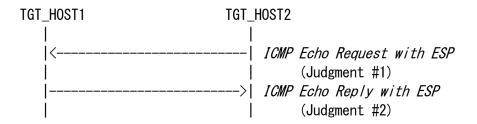
IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



5.4.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that can select ICMP

Type as SPD selector if you choose End-Node vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC4301]

[RFC4303]

- [RFC4443]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOST1			
HOST2_SA1-0	>	HOST1_SA1-I	ICMPv6	Echo	Request
HOST2_SA1-I	<	HOST1_SA1-0	ICMPv6	Echo	Request
HOST2_SA2-0	>	HOST1_SA2-I	ICMPv6	Echo	Reply
HOST2 SA2-I	<	HOST1 SA2-0	ICMPv6	Echo	Reply



Security Association Database (SAD) for HOST1_SA1-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des2to1req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1req

Security Policy Database (SPD) for $HOST1_SA1-I$

TGT_HOST2_Link1
TGT_HOST1_Link0
TGT_HOST2_Link1
TGT_HOST1_Link0
ICMPv6 Echo Request
in
ESP
tunnel

Security Association Database (SAD) for $HOST1_SA1-0$

TOT 1100T4 1 : 1 0
TGT_HOST1_Link0
TGT_HOST2_Link1
0x2000
tunne l
ESP
3DES-CBC
ipv6readylogo3des1to2req
HMAC-SHA1
ipv6readysha11to2req

Security Policy Database (SPD) for $HOST1_SA1-0$

tunnel source address	TGT_H0ST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA1-I

coda ity necestation bacasace (en	, 101 110012 <u>-</u> 0,11 1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST2_SA1-I

	_
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA1-0

	<u> </u>
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des2to1req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1req

Security Policy Database (SPD) for HOST2_SA1-0

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_H0ST1_Link0
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST1_SA2-I

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD) for HOST1_SA2-I

TGT_H0ST2_Link1
TGT_HOST1_LinkO
TGT_HOST2_Link1
TGT_HOST1_Link0
ICMPv6 Echo Reply
in
ESP
tunnel

Security Association Database (SAD) for HOST1_SA2-0

700001 10 70000 10 10 10 10 10 10 10 10 10 10 10 10	
source address	TGT_HOST1_LinkO
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST1_SA2-0

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_H0ST2_Link1
source address	TGT_HOST1_LinkO
destination address	TGT_H0ST2_Link1
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA2-I

• • • • • • • • • • • • • • • • • • • •	-
source address	TGT_HOST1_Link0
destination address	TGT_H0ST2_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST2_SA2-I

Total ity it is parabase (e.p., it is	
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA2-0

	_
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD) for HOST2_SA2-0

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP1 tunnel

IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1req
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP1 tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des1to2rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2rep
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



ICMP Echo Request within ESP2 tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Туре	128 (Echo Request)

ICMP Echo Reply within ESP2 tunnel

IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	129 (Echo Reply)



Procedure:

TGT_HOST1 TG	TGT_HOST2		
 < ;	 - ICMP Echo Request with ESP1 (Judgment #1) > ICMP Echo Reply with ESP1 (Judgment #2)		
	ICMP Echo Request with ESP2 (Judgment #3)		
<	- <i>ICMP Echo Reply with ESP2</i> (Judgment #4)		

- 1. TGT_HOST2 sends "ICMP Echo Request with ESP1" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP1"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2
- 6. TGT_HOST1 sends "ICMP Echo Request with ESP2" to TGT_HOST2
- 7. Observe the packet transmitted by TGT_HOST1
- 8. TGT_HOST2 sends "ICMP Echo Reply with ESP2"
- 9. Observe the packet transmitted by TGT_HOST2
- 10. Save the command \log on TGT_HOST1



Judgment:

Judgment #1 Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP1" Judgment #2 Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP1"

Judgment #3

Step-7: TGT_HOST2 transmits "ICMP Echo Request with ESP2"

Judgment #4

Step-9: TGT_HOST1 transmits "ICMP Echo Reply with ESP2"

Possible Problems:

TGT_HOST1 or TGT_HOST2 may be a passive node which does not implement an application for sending Echo Requests. One of the following method to perform this test is required for the passive node.

- c) using UDP application to invoke ICMPv6 Destination Unreachable (Port unreachable) (see Appendix-D Section 1.1)
- d) invoking Neighbor Unreachability Detection (see Appendix-D Section 1.2)



5.4.9. Tunnel Mode: dummy packet handling

Purpose:

Verify that device can handle dummy packet as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support dummy packet

handling if you choose End-Node vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOST1
HOST2_SA-0	>	HOST1_SA-I
HOST2_SA-I	<	HOST1_SA-0



Security Association Database (SAD) for HOST1 SA-I

decar tely medecial teleparate (emb) for medit_em 1		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_HOST2_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

Security Association Database (SAD) for $HOST1_SA-0$

•	—
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

Total 10) Modern Buttabase (emb) 101 Modit_em 1		
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for HOST2_SA-I

	_
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA-0

	
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_LinkO
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

Source Address	TGT_HOST2_Link1
Destination Address	TGT_HOST1_Link0
SPI	0x1000
Algorithm	3DES-CBC
Key	ipv6readylogo3descbc2to1
Authentication Algorithm	HMAC-SHA1
Authentication Key	ipv6readylogsha12to1
Source Address	TGT_HOST2_Link1
Destination Address	TGT_HOST1_Link0
Type	128 (Echo Request)
	Destination Address SPI Algorithm Key Authentication Algorithm Authentication Key Source Address Destination Address

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



dummy packet 1

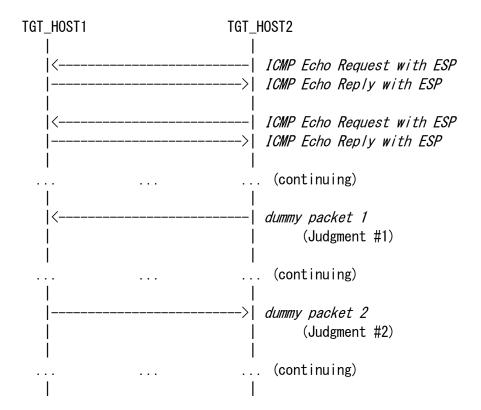
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	Next Header	59 (no next header)

dummy packet 2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_H0ST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	Next Header	59 (no next header)



Procedure:



- 1. TGT_HOST2 keeps sending "ICMP Echo Request with ESP" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "dummy packet 1"

Judgment #2

Step-3: TGT_HOST1 transmits "dummy packet 2" $\,$

Possible Problems:

None.



5.4.10. Tunnel Mode: TFC padding

Purpose:

Verify that device can handle TFC padding as part of traffic flow confidentiality

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support TFC padding

if you choose End-Node vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC4303]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOS	ST1
HOST2_SA-0	>	HOST1_	_SA-I
HOST2_SA-I	<	HOST1_	_SA-0



Security Association Database (SAD) for HOST1_SA-I

Total 1 to 1 t		
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for $HOST1_SA-I$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $HOST1_SA-O$

• • • • • • • • • • • • • • • • • • • •	-
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2_SA-I

coda ity incocoración bacabaco (en	, 10. 110012 <u>-</u> 071 1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

	_
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA-0

	
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_H0ST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_H0ST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



ICMP Echo Request within TFC padded ESP tunnel

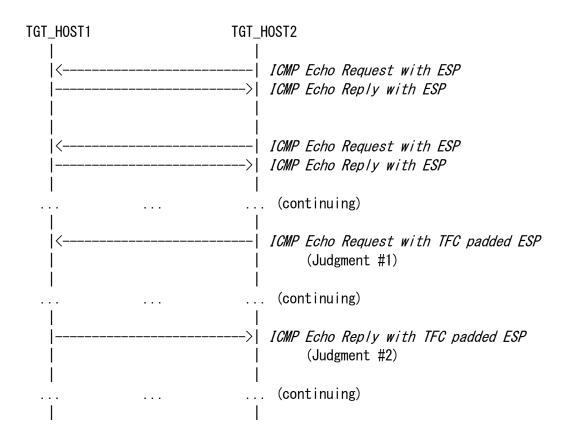
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within TFC padded ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
	TFC padding	any size other than 0 byte
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 keeps sending "ICMP Echo Request with ESP" to TGT_HOST1 at time enough to confirm randomness of the event
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. Otherwise, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with TFC padded ESP"

Judgment #2

Step-3: TGT_HOST1 transmits "ICMP Echo Reply with TFC padded ESP"

Possible Problems:

None.



5.4.11. Tunnel Mode: Fragmentation

Purpose:

Verify that device can handle ICMPv6 Error Message (Packet Too Big) and packet fragmentation/reassembly.

Category:

End-Node: BASIC (A requirement for all End-Node NUTs if you choose End-Node vs.

End-Node Tunnel Mode)

: N/A SGW

References:

- [RFC2404]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_H0ST2	TGT_HOST1
HOST2_SA-0>	HOST1_SA-I
HOST2_SA-I <	HOST1_SA-0



Security Association Database (SAD) for HOST1_SA-I

Total 1 to 7 house and the standard (chip) 1 of house 1_on 1		
source address	TGT_H0ST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc2to1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha12to1	

Security Policy Database (SPD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	Any
direction	In
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA-0

• • • • • • • • • • • • • • • • • • • •	_
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-0

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2 SA-I

Coodiney house action bacasacs (ons) for house_on 1		
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbc1to2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha11to2	

Security Policy Database (SPD) for $HOST2_SA-I$

	-
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA-0

· · · · · · · · · · · · · · · · · · ·	—
source address	TGT_H0ST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-0

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

Fragmented ICMP Echo Request within ESP 1

	· ·	
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

Fragmented ICMP Echo Request within ESP 2

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Request



ICMP Echo Reply within ESP

I chini Ecite Hept	, =	
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
	Payload Length	1460
ICMP	Type	129 (Echo Reply)

ICMP Error Message (Packet Too Big)

IP Header	Source Address	REF_ROUTER1
	Destination Address	TGT_HOST1
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply with
		ESP



Fragmented ICMP Echo Reply within ESP 1

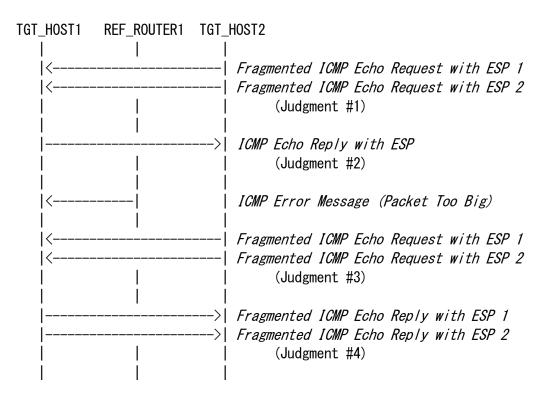
IP Header	Source Address	TGT_H0ST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
	Payload Length	1stPL (= MTU-40) (e.g. 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	129 (Echo Reply)

Fragmented ICMP Echo Reply within ESP 2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
	Payload Length	2ndPL (= 1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of ICMP Echo Reply



Procedure:



- 1. TGT_HOST2 transmits "Fragmented ICMP Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted by TGT HOST2
- 3. Observe the packet transmitted by TGT_HOST1
- 4. TGT HOST2 transmits "Fragmented ICMP Echo Request" to TGT HOST1
- 5. Observe the packet transmitted by TGT_HOST2
- 6. Observe the packet transmitted by TGT_HOST1
- 7. Save the command log on TGT_HOST2
- 8. Disconnect TGT_HOST1 and TGT_HOST2. Connect TGT_HOST2 to LinkO. Connect TGT_HOST1 to Link1. Switch the roles of TGT_HOST1 and TGT_HOST2. Repeat step 1 to step 7

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "Fragmented ICMP Echo Request with ESP"

Judgment #2

Step-3: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Judgment #3

Step-5: TGT_HOST2 transmits "Fragmented ICMP Echo Request with ESP"

Judgment #4

 ${\tt Step-6: TGT_HOST1 \ transmits} \ \textit{``Fragmented ICMP Echo Reply with ESP''}$

Possible Problems:

None.



5.4.12. Tunnel Mode: ESP=3DES-CBC HMAC-SHA-256

Purpose:

Tunnel mode between two End-Nodes, ESP=3DES-CBC HMAC-SHA-256

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs that support

HMAC-SHA-256 as an authentication algorithm if you choose End-Node

vs. End-Node Tunnel Mode)

SGW : N/A

References:

- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4868]

Initialization:

Use common topology described as Fig. 1 Set NUT's SAD and SPD as following:

TGT_HOST2		TGT_HOS	T1
HOST2_SA-0	>	HOST1_	SA-I
HOST2_SA-I	<	HOST1_	SA-0



Security Association Database (SAD) for HOST1_SA-I

cocal feet factor bacasace (chis) fe	
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha22562to1

Security Policy Database (SPD) for $HOST1_SA-I$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_LinkO
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for $HOST1_SA-O$

	· —
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	HMAC-SHA-256
ESP authentication key	ipv6readylogoph2ipsecsha22561to2

Security Policy Database (SPD) for $HOST1_SA-0$

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Security Association Database (SAD) for HOST2 SA-I

Total Its Modern Batabase (OND) Tot Modificant I			
TGT_HOST1_Link0			
TGT_HOST2_Link1			
0x2000			
tunnel			
ESP			
3DES-CBC			
ipv6readylogo3descbc1to2			
HMAC-SHA-256			
ipv6readylogoph2ipsecsha22561to2			

Security Policy Database (SPD) for HOST2_SA-I

	_
tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA-0

- COCALLEY MODOCIALION BACABAGO (CMB) TOT MODIL_ON C			
source address	TGT_HOST2_Link1		
destination address	TGT_HOST1_Link0		
SPI	0x1000		
mode	tunnel		
protocol	ESP		
ESP algorithm	3DES-CBC		
ESP algorithm key	ipv6readylogo3descbc2to1		
ESP authentication	HMAC-SHA-256		
ESP authentication key	ipv6readylogoph2ipsecsha22562to1		

Security Policy Database (SPD) for $HOST2_SA-0$

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_LinkO
upper spec	any
direction	Out
protocol	ESP
mode	tunnel



Packets:

ICMP Echo Request within ESP tunnel

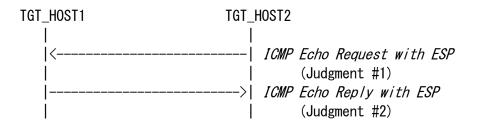
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha22562to1
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	HMAC-SHA-256
	Authentication Key	ipv6readylogoph2ipsecsha2251to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)



Procedure:



- 1. TGT_HOST2 sends "ICMP Echo Request with ESP" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST2
- 3. TGT_HOST1 sends "ICMP Echo Reply with ESP"
- 4. Observe the packet transmitted by TGT_HOST1
- 5. Save the command log on TGT_HOST2

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll. If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMP Echo Request with ESP"

Judgment #2

Step-4: TGT_HOST1 transmits "ICMP Echo Reply with ESP"

Possible Problems:

None.



Appendix-A Required Data

When you apply for an IPv6 Ready Logo Phase-2(IPsec) you need to submit test logs. In this appendix the detail requirement for the test log is described.

1.1. Required Data Type

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

A) Topology map

Network topology figures or address list, with IPv6 addresses and MAC address of each attached interfaces, are required. Fig. 4 is an example of topology figure.

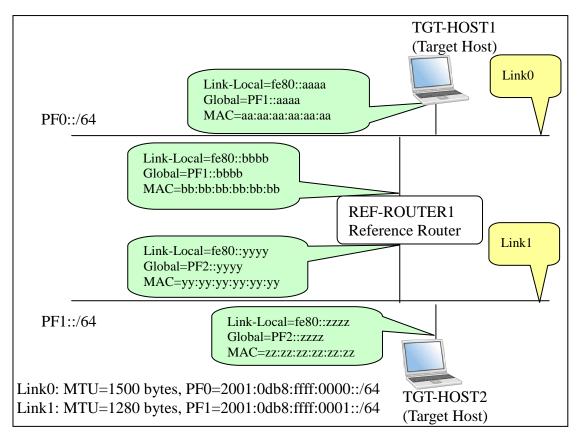




Fig. 4 Topology map example

Fig. 5 is an example of address list.

TGT_HOST1:

Link-Local=fe80::aaaa Global=PF1::aaaa

MAC=aa:aa:aa:aa:aa

REF_ROUTER1 [Link0]:

Link-Local=fe80::bbbb Global=PF1::bbbb

MAC=bb:bb:bb:bb:bb

REF_ROUTER1 [Link1]:

Link-Local=fe80::yyyy

Global=PF2::yyyy

MAC=yy:yy:yy:yy:yy

TGT HOST2:

Link-Local=fe80::zzzz

Global=PF2::zzzz

 $MAC \!\!=\!\! zz \!\!:\!\! zz \!\!:\!\!$

Fig. 5 Address List example

B) Command Log

Ping is used as default application. When you run test with ping application, please save the command log into individual files.

We allow using other protocol than ICMP Echo Request and Reply. Even though you use other kind of application, please save the command log.

Save the command files for each test on each node.

C) Packet Capture File

Capture all packets on each link during the test with a device that is not part of the test.

Make individual topdump(pcap) format file for each test and link or put



the packet dump in a readable HTML file.

If you run topdump, please specify packet size as 4096.

e.g.,) tcpdump -i if0 -s 4096 -w 5.1.A. VendorA. Link0. dump

D) Test Result Table

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.



E) Keying Information

Collect all SPD and SAD information. If you configure keying information manually, it is not required to submit keying information. Fig. 6 is an example of Keying Information.

TGT_HOST1's SAD1:

Source Address: TGT_HOST1_Link0
Destination Address: TGT_HOST2_Link1

SPI: 0x1000 mode: transport protocol: ESP

ESP algorithm: 3DES-CBC

ESP key: ipv6readylogo3descbc1to2 ESP authentication: HMAC-SHA1

ESP authentication key: ipv6readylogsha11to2

TGT_HOST1's SAD2:

Source Address: TGT_HOST2_Link1
Destination Address: TGT_HOST1_Link0

SPI: 0x2000 mode: transport protocol: ESP

ESP algorithm: 3DES-CBC

ESP key: ipv6readylogo3descbc2to1 ESP authentication: HMAC-SHA1

ESP authentication key: ipv6readylogsha12to1

TGT_HOST1's SPD1:

Source Address: TGT_HOST1_Link0
Destination Address: TGT_HOST2_Link1

upper spec: any direction: out protocol: ESP mode: transport

TGT_HOST1's SPD2:

Source Address: TGT_HOST1_Link0
Destination Address: TGT_HOST2_Link1

upper spec: any direction: in protocol: ESP mode: transport

Fig. 6 Keying Information example



1.2. Data file name syntax

Please use following syntax in the file name.

A) Topology Map

Syntax: Chapter. Section. Sub_section. ON. topology

For "0N", use the Node's vendor name which behaved as a Opposite side target Node (0N).

e.g.,)

5.1.1 Transport Mode ESP=3DES-CBC HMAC-SHA1

TGT_HOST1 (Your Device):

End-Node [vendor: VendorX, model: rHost1, version: 1.0]

TGT_HOST2 (Opposite side device):

End-Node [vendor: VendorA, model: rHost2, version: 2.0]

5. 1. 1. Vendor A. topology

B) Command Results

Syntax: Chapter. Section. Sub_Section. SRC. DST. result

For "SRC", use the vendor name on which the commands were run. If SRC is a Reference Host, just specify REF_HOSTn as SRC. For "DST", use the vendor name to which the commands were run, in other word, destination of ping command. If DST is a Reference Host, just specify REF_HOSTn as DST

e.g.,)

Typical Naming sample are following.

5. 1. 1 Transport Mode ESP=3DES-CBC HMAC-SHA1

TGT_HOST1: End-Node [vendor: VendorA, model: rHost1, version: 1.0]
TGT_HOST2: End-Node [vendor: VendorB, model: rHost2, version: 2.0]



5. 1. 1. VendorB. VendorA. result

5. 2. 1 Tunnel Mode ESP=3DES-CBC HMAC-SHA1

TGT_SGW1: SGW [vendor: VendorA, model: rRouter1, version: 1.0]
TGT_SGW2: SGW [vendor: VendorB, model: rRouter2, version: 2.0]
REF_HOST1: Host [vendor: VendorC, model: rHost1, version: 1.0]
REF_HOST2: Host [vendor: VendorD, model: rHost2, version: 2.0]

5. 2. 1. REF_HOST2. REF_HOST1. result

C) Captured packet file

Syntax: Chapter. Section. Sub_Section. ON. Link. dump

For "Link", use the captured link name.

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

Even if the command run on a Reference Node, you should list ON's vendor name rather than REF_HOST*n*.

e.g.,)

5.1.1 Transport Mode ESP=3DES-CBC HMAC-SHA1

TGT_HOST1 (Your Device):

End-Node [vendor: VendorX, model: rHost1, version: 1.0]

TGT_HOST2 (Opposite side device):

End-Node [vendor: VendorA, model: rHost2, version: 2.0]

5. 1. 1. Vendor A. Link O. dump

5. 1. 1. Vendor A. Link 1. dump

D) Test Result Table

Syntax: Vendor. table

In this file you must make table for each sub-section.



For End-Node)

- Transport Mode (BASIC): Test 5.1.X is required.

For Test 5.1.X

1 01 1050 5.1.21		
	VendorA	VendorB
	(End-Node)	(End-Node)
Applicants_name		
(End-Node)		

- Tunnel Mode (ADVANCED): Test 5.3.X or Test 5.4.X is required.

or

For Test 5.3.X

1 01 1050 5.5.71		
	VendorC (SGW)	VendorD (SGW)
Applicants_name (End Node)		

For Test 5.4.X

	VendorC (End Node)	VendorD (End Node)
Applicants_name (End Node)		

For SGW)

- Tunnel Mode (BASIC): Test 5.2.X or Test 5.3.X is required.

For Test 5.2.X

	VendorA (SGW)	VendorB (SGW)
Applicants_name (SGW)		

For Test 5.3.X

	1 01 1000 0 10 11 1		
		VendorA	VendorB
		(End-Node)	(End-Node)
L	Applicants_name		
	(SGW)		

e.g.,)

Test result of following host.

TGT_HOST1:

End-Node [vendor: VendorX, model: rHost1, version: 1.0]
VendorX.table

E) Keying Information

Syntax: Chapter. Section. Sub_Section. ON. key

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

e.g.,)



5.1.1 Transport Mode ESP=3DES-CBC HMAC-SHA1

TGT_HOST1 (Your Device):

End-Node [vendor: VendorX, model: rHost1, version: 1.0]

TGT_HOST2 (Opposite side device):

End-Node [vendor: VendorA, model: rHost2, version: 2.0]

5. 1. 1. Vendor A. key



1.3. Data Archive

Please organize your data as following directory structure.

```
$YourDeviceName_ver/
Conformance/
Interoperability/
```

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 all files under "\$YourDeviceName_ver" in it.

1) File list for End-Node

1-1) In the case of supporting only transport mode

Test 5.1 is performed with following condition.

TGT_HOST1:

Your device:	VendorX (End Node)	7
rour device:	r vendora (end Node)	,

TGT_HOST2:

Counterpart End Node 1:	VendorA
Counterpart End Node 2:	VendorB

The file list is described below.



```
5. 1. 1. VendorA. topology
       5. 1. 1. VendorA. key
   5. 1. [2-7]/, 5. 1. 9/, 5. 1. 10/, 5. 1. 12/
       5. 1. X. VendorA. LinkO. dump
       5. 1. X. Vendor A. Link 1. dump
       5. 1. X. VendorA. VendorX. result
       5. 1. X. VendorA. topology
       5. 1. X. VendorA. key
   5. 1. 8/, 5. 1. 11/
       5. 1. Y. Vendor A. Link O. dump
       5. 1. Y. Vendor A. Link 1. dump
       5. 1. Y. Vendor A. Vendor X. result
       5. 1. Y. VendorX. VendorA. result
       5. 1. Y. VendorA. topology
       5. 1. Y. VendorA. key
End-Node. VendorB/
   5. 1. 1/
       5. 1. 1. VendorB. LinkO. dump
       5. 1. 1. VendorB. Link1. dump
       5. 1. 1. VendorB. VendorX. result
       5. 1. 1. VendorB. topology
       5. 1. 1. VendorB. key
   5. 1. [2-7]/, 5. 1. 9/, 5. 1. 10/, 5. 1. 12/
       5. 1. X. VendorB. LinkO. dump
       5. 1. X. VendorB. Link1. dump
       5. 1. X. VendorB. VendorX. result
       5. 1. X. VendorB. topology
       5. 1. X. VendorB. key
   5. 1. 8/, 5. 1. 11/
       5. 1. Y. VendorB. LinkO. dump
       5. 1. Y. VendorB. Link1. dump
       5. 1. Y. VendorB. VendorX. result
       5. 1. Y. VendorX. VendorB. result
       5. 1. Y. VendorB. topology
       5. 1. Y. VendorB. key
VendorX.table
```

1-2) In the case of supporting transport mode and tunnel mode

1-2-1) In the case of choosing SGW as the counterpart device

Test 5.1 is performed with following condition.

TGT_HOST1:

Your device: VendorX (End Node)



TGT_HOST2:

Counterpart End Node 1:	VendorA
Counterpart End Node 2:	VendorB

Test 5.3 is performed with following condition.

TGT_HOST1:

Your device: VendorX (End Node)

TGT_SGW1:

Counterpart SGW 1:	VendorC
Counterpart SGW 2:	VendorD

The file list is described below.

\${Your_Device_ver}/				
Conformance/				
Interoperability/				
End-Node. VendorA/				
5.1.1/				
5.1.1. VendorA. VendorX. result				
5.1.1. VendorA. topology				
5.1.[2-7]/, 5.1.9/, 5.1.10/, 5.1.12/				
5.1.X. VendorA. LinkO. dump				
5.1.X. VendorA. VendorX. result				
5.1.X. VendorA. topology				
5. 1. 8/, 5. 1. 11/				
5.1.Y. VendorA. LinkO. dump				
5.1.Y. VendorA. Link1. dump				
5.1.Y. VendorA. VendorX. result				
5.1.Y. VendorX. VendorA. result				
5.1.Y. VendorA. topology				
5. 1. Y. VendorA. key				
Fr. J. N. J. V. v. J. v.D./				
End-Node. VendorB/ 				
5. 1. 1. VendorB. Link0. dump				
5.1.1. VendorB. Link1. dump				
5.1.1. VendorB. VendorX. result				



```
5. 1. 1. VendorB. topology
    5. 1. 1. VendorB. key
   5. 1. [2-7]/, 5. 1. 9/, 5. 1. 10/, 5. 1. 12/
     5. 1. X. VendorB. LinkO. dump
       5. 1. X. VendorB. Link1. dump
       5. 1. X. VendorB. VendorX. result
      5. 1. X. VendorB. topology
      5. 1. X. VendorB. key
   5. 1. 8/, 5. 1. 11/
      5. 1. Y. VendorB. LinkO. dump
       5. 1. Y. VendorB. Link1. dump
       5. 1. Y. VendorB. VendorX. result
       5. 1. Y. VendorX. VendorB. result
       5. 1. Y. VendorB. topology
     5. 1. Y. VendorB. key
SGW. VendorC/
 5. 3. 1/
      5. 3. 1. VendorC. LinkO. dump
      5. 3. 1. VendorC. Link1. dump
       5. 3. 1. VendorC. Link2. dump
       5. 3. 1. REF_HOST2. VendorX. result
       5. 3. 1. VendorC. topology
      5.3.1. VendorC. key
   5. 3. [2-7]/, 5. 3. 9/, 5. 3. 10/, 5. 3. 11/, 5. 3. 12/
      5. 3. X. VendorC. LinkO. dump
       5. 3. X. VendorC. Link1. dump
       5. 3. X. VendorC. Link2. dump
       5. 3. X. REF_HOST2. VendorX. result
       5. 3. X. VendorC. topology
     5. 3. X. VendorC. key
   5. 3. 8/
      5. 3. 8. VendorC. LinkO. dump
       5. 3. 8. VendorC. Link1. dump
      5. 3. 8. VendorC. Link2. dump
      5. 3. 8. REF_HOST2. VendorX. result
       5. 3. 8. VendorX. REF_HOST2. result
       5. 3. 8. VendorC. topology
     5. 3. 8. VendorC. key
SGW. VendorD/
 5. 3. 1/
      5. 3. 1. VendorD. LinkO. dump
       5. 3. 1. VendorD. Link1. dump
       5. 3. 1. VendorD. Link2. dump
       5. 3. 1. REF_HOST2. VendorX. result
       5. 3. 1. VendorD. topology
      5. 3. 1. VendorD. key
   5. 3. [2-7]/, 5. 3. 9/, 5. 3. 10/, 5. 3. 11/, 5. 3. 12/
```



```
5. 3. X. VendorD. LinkO. dump
      5. 3. X. VendorD. Link1. dump
      5. 3. X. VendorD. Link2. dump
      5. 3. X. REF_HOST2. VendorX. result
       5. 3. X. VendorD. topology
      5. 3. X. VendorD. key
   5. 3. 8/
       5. 3. 8. VendorD. LinkO. dump
       5. 3. 8. VendorD. Link1. dump
      5. 3. 8. VendorD. Link2. dump
       5. 3. 8. REF_HOST2. VendorX. result
      5. 3. 8. VendorX. REF_HOST2. result
      5.3.8. VendorD. topology
     5. 3. 8. VendorD. key
VendorX.table
```

1-2-2) In the case of choosing End-Node as the counterpart device

Test 5.1 is performed with following condition.

TGT HOST1:

Your device: VendorX (End Node)

TGT_HOST2:

Counterpart End Node 1 for the transport mode:	
Counterpart End Node 2 for the transport mode:	VendorB

Test 5.4 is performed with following condition.

TGT HOST1:

Your device: VendorX (End Node)

TGT_HOST2:

Counterpart End Node 3 for the tunnel mode:	VendorC
Counterpart End Node 4 for the tunnel mode:	VendorD

The file list is described below.

```
${Your_Device_ver}/
  Conformance/
   | ...
  Interoperability/
    | End-Node. VendorA/
```



```
5. 1. 1/
       5. 1. 1. VendorA. LinkO. dump
       5. 1. 1. Vendor A. Link 1. dump
       5. 1. 1. VendorA. VendorX. result
       5. 1. 1. VendorA. topology
       5. 1. 1. VendorA. key
   5. 1. [2-7]/, 5. 1. 9/, 5. 1. 10/, 5. 1. 12/
       5. 1. X. Vendor A. Link O. dump
       5. 1. X. Vendor A. Link 1. dump
       5. 1. X. VendorA. VendorX. result
       5. 1. X. VendorA. topology
     5. 1. X. VendorA. key
   5. 1. 8/, 5. 1. 11/
       5. 1. Y. VendorA. LinkO. dump
       5. 1. Y. Vendor A. Link 1. dump
       5. 1. Y. Vendor A. Vendor X. result
       5. 1. Y. VendorX. VendorA. result
       5. 1. Y. VendorA. topology
       5. 1. Y. VendorA. key
End-Node. VendorB/
   5. 1. 1/
      5. 1. 1. VendorB. LinkO. dump
       5. 1. 1. VendorB. Link1. dump
       5. 1. 1. VendorB. VendorX. result
       5. 1. 1. VendorB. topology
       5. 1. 1. VendorB. key
   5. 1. [2-7]/, 5. 1. 9/, 5. 1. 10/, 5. 1. 12/
       5. 1. X. VendorB. LinkO. dump
       5. 1. X. VendorB. Link1. dump
       5. 1. X. VendorB. VendorX. result
       5. 1. X. VendorB. topology
     5. 1. X. VendorB. key
   5. 1. 8/, 5. 1. 11/
       5. 1. Y. VendorB. LinkO. dump
       5. 1. Y. VendorB. Link1. dump
       5. 1. Y. VendorB. VendorX. result
       5. 1. Y. VendorX. VendorB. result
       5. 1. Y. VendorB. topology
     5. 1. Y. VendorB. key
End-Node. VendorC/
 5. 4. 1/
     5. 4. 1. VendorC. LinkO. dump
       5. 4. 1. VendorC. Link1. dump
       5. 4. 1. VendorC. VendorX. result
       5. 4. 1. VendorC. topology
       5. 4. 1. VendorC. key
   5. 4. [2-7]/, 5. 4. 9/, 5. 4. 10/, 5. 4. 12/
```



```
5. 4. X. VendorC. LinkO. dump
       5. 4. X. VendorC. Link1. dump
       5. 4. X. VendorC. VendorX. result
       5. 4. X. VendorC. topology
       5. 4. X. VendorC. key
   5. 4. 8/, 5. 4. 11/
       5. 4. Y. VendorC. LinkO. dump
       5. 4. Y. VendorC. Link1. dump
       5. 4. Y. Vendor C. Vendor X. result
       5. 4. Y. VendorX. VendorC. result
       5. 4. Y. VendorC. topology
       5. 4. Y. VendorC. key
End-Node. VendorD/
   5. 4. 1/
       5. 4. 1. VendorD. LinkO. dump
       5. 4. 1. VendorD. Link1. dump
       5. 4. 1. VendorD. VendorX. result
       5. 4. 1. VendorD. topology
    5. 4. 1. VendorD. key
   5. 4. [2-7]/, 5. 4. 9/, 5. 4. 10/, 5. 4. 12/
       5. 4. X. VendorD. LinkO. dump
       5. 4. X. VendorD. Link1. dump
       5. 4. X. VendorD. VendorX. result
       5. 4. X. VendorD. topology
    5. 4. X. VendorD. key
   5. 4. 8/, 5. 4. 11/
       5. 4. Y. VendorD. LinkO. dump
       5. 4. Y. VendorD. Link1. dump
       5. 4. Y. VendorD. VendorX. result
       5. 4. Y. VendorX. VendorD. result
       5. 4. Y. VendorD. topology
     5. 4. Y. VendorD. key
VendorX.table
```

2) File list for SGW

2-1) In the case of choosing SGW as the counterpart device

Test 5.2 is performed with following condition.

TGT_SGW1/TGT_SGW2:

Your device: VendorX (SGW)

TGT_SGW1/TGT_SGW2:

Counterpart SGW 1:	VendorA
Counterpart SGW 2:	VendorB



The file list is described below.

```
${Your_Device_ver}/
   Conformance/
     | ...
   Interoperability/
       SGW. VendorA/
          5, 2, 1/
              5. 2. 1. VendorA. LinkO. dump
              5. 2. 1. VendorA. Link1. dump
              5. 2. 1. Vendor A. Link 2. dump
              5. 2. 1. VendorA. Link3. dump
              5. 2. 1. REF_HOST2. REF_HOST1. result
              5. 2. 1. VendorA. topology
              5. 2. 1. VendorA. key
          5. 2. [2-7]/, 5. 2. 9/, 5. 2. 10/, 5. 2. 12/
              5. 2. X. VendorA. LinkO. dump
              5. 2. X. VendorA. Link1. dump
              5. 2. X. VendorA. Link2. dump
              5. 2. X. VendorA. Link3. dump
              5. 2. X. REF_HOST2. REF_HOST1. result
              5. 2. X. VendorA. topology
              5. 2. X. VendorA. key
          5. 2. 8/, 5. 2. 11/
              5. 2. Y. Vendor A. Link O. dump
              5. 2. Y. Vendor A. Link 1. dump
              5. 2. Y. Vendor A. Link 2. dump
              5. 2. Y. Vendor A. Link 3. dump
              5. 2. Y. REF_HOST2. REF_HOST1. result
              5. 2. Y. REF_HOST1. REF_HOST2. result
              5. 2. Y. VendorA. topology
              5. 2. Y. VendorA. key
      SGW. VendorB/
          5. 2. 1/
              5. 2. 1. VendorB. LinkO. dump
              5. 2. 1. VendorB. Link1. dump
              5. 2. 1. VendorB. Link2. dump
              5. 2. 1. VendorB. Link3. dump
              5. 2. 1. REF_HOST2. REF_HOST1. result
              5. 2. 1. VendorB. topology
           5. 2. 1. VendorB. key
          5. 2. [2-7]/, 5. 2. 9/, 5. 2. 10/, 5. 2. 12/
              5. 2. X. VendorB. LinkO. dump
              5. 2. X. VendorB. Link1. dump
              5. 2. X. VendorB. Link2. dump
```



2-2) In the case of choosing End-Node as the counterpart device

Test 5.3 is performed with following condition.

TGT SGW1:

Your device: VendorX (SGW)

TGT_HOST1:

Counterpart End-Node 1:	VendorA
Counterpart End-Node 2:	VendorB

The file list is described below.

```
${Your_Device_ver}/
   Conformance/
   | ...
   Interoperability/
      End-Node. VendorA/
         5. 3. 1/
          5. 3. 1. VendorA. LinkO. dump
             5. 3. 1. VendorA. Link1. dump
             5. 3. 1. VendorA. Link2. dump
             5. 3. 1. REF_HOST2. VendorA. result
             5. 3. 1. VendorA. topology
          5. 3. 1. VendorA. key
       5.3.[2-7]/, 5.3.9/, 5.3.10/, 5.3.11/, 5.3.1.2/
             5. 3. X. VendorA. LinkO. dump
             5. 3. X. Vendor A. Link 1. dump
             5. 3. X. VendorA. Link2. dump
             5. 3. X. REF_HOST2. VendorA. result
```



```
5. 3. X. VendorA. topology
     5. 3. X. VendorA. key
   5.3.8/
       5. 3. 8. VendorA. LinkO. dump
       5. 3. 8. VendorA. Link1. dump
       5. 3. 8. VendorA. Link2. dump
       5. 3. 8. REF_HOST2. VendorA. result
       5. 3. 8. VendorA. REF_HOST2. result
       5.3.8. VendorA. topology
     5.3.8. VendorA. key
End-Node. VendorB/
 5. 3. 1/
     5.3.1. VendorB. LinkO. dump
       5. 3. 1. VendorB. Link1. dump
       5. 3. 1. VendorB. Link2. dump
       5. 3. 1. REF_HOST2. VendorB. result
       5. 3. 1. VendorB. topology
     5. 3. 1. VendorB. key
   5. 3. [2-7]/, 5. 3. 9/, 5. 3. 10/, 5. 3. 11/, 5. 3. 12/
       5. 3. X. VendorB. LinkO. dump
       5. 3. X. VendorB. Link1. dump
       5. 3. X. VendorB. Link2. dump
       5. 3. X. REF_HOST2. VendorB. result
       5. 3. X. VendorB. topology
     5. 3. X. VendorB. key
   5.3.8/
       5. 3. 8. VendorB. LinkO. dump
       5. 3. 8. VendorB. Link1. dump
       5. 3. 8. VendorB. Link2. dump
       5. 3. 8. REF_HOST2. VendorB. result
       5. 3. 8. VendorB. REF_HOST2. result
       5. 3. 8. VendorB. topology
     5. 3. 8. VendorB. key
VendorX.table
```



Appendix-B annex-5.1.8 for the passive node

This appendix describes alternative methods to perform Test 5.1.8 on the passive node which doesn't have the application to send ICMPv6 Echo Request.

In these method, only TGT_HOST2 role can be the passive node. If TGT_HOST1 is the passive node, switch the role such that TGT_HOST2 is the passive node.



1.1.using UDP application to invoke ICMPv6 Destination

Unreachable (Port unreachable)

Requirements:

- TGT_HOST1
 - ♦ Must support the application to send ICMPv6 Echo Request
 - ♦ Must support the application to send UDP packet (e.g., DNS lookup client)
- TGT_HOST2 (passive node)
 - ♦ Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply
 - ♦ Must respond to UDP packet toward the closed port with ICMPv6 Destination Unreachable (Port unreachable)

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
(passive node)
 TGT_HOST1 ----- transport ----- TGT_HOST2
HOST1\_SA1-O ----- spi=0x1000 ----> HOST2\_SA1-I ICMPv6 Echo Request
HOST1_SA2-I <---- spi=0x2000 ----- HOST2_SA2-0 ICMPv6 Echo Reply
HOST1_SA3-I <---- spi=0x3000 ----- HOST2_SA3-0
                                                ICMPv6 Destination Unreachable
                                                (Port unreachable)
```



HOST1_SA1-O and HOST2_SA1-I

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD)

	HOST1_SA1-O	HOST2_SA1-I
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
upper spec	ICMPv6 Echo Request	
direction	outbound inbound	
protocol	ESP	
mode	transport	

HOST1_SA2-I and HOST2_SA2-O

Security Association Database (SAD)

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

	HOST1_SA2-I	HOST2_SA2-O
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Echo Reply	
direction	inbound outbound	
protocol	ESP	
mode	transport	



HOST1_SA3-I and HOST2_SA3-O

Security Association Database (SAD)

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1dst
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1dst

	HOST1_SA3-I	HOST2_SA3-O
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Destination Unreachable	
direction	inbound outbound	
protocol	ESP	
mode	transport	



Packets:

ICMPv6 Echo Request with ESP1

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
ICMPv6	Type	128 (Echo Request)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
ICMPv6	Type	129 (Echo Reply)

UDP packet toward closed port

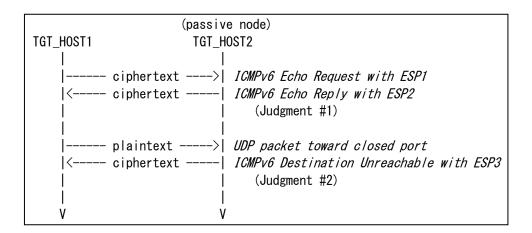
	IPv6	Source Address	TGT_HOST1_Link0
		Destination Address	TGT_HOST2_Link1
Π	UDP	Source Port	Any unused port on TGT_HOST1
		Destination Port	Any closed port on TGT_HOST2

ICMPv6 Destination Unreachable with ESP3

IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1dst
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1dst
ICMPv6	Type	1 (Destination Unreachable)
	Code	4 (Port unreachable)



Procedure:



- 1. TGT_HOST1 sends "ICMPv6 Echo Request with ESP1" to TGT_HOST2
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Save the command log on TGT_HOST1
- 4. TGT_HOST1 sends "UDP packet toward closed port" to TGT_HOST2
- 5. Observe the packet transmitted by TGT_HOST2
- 6. Save the command log on TGT_HOST1

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMPv6 Echo Reply with ESP2"

Judgment #2

Step-5: TGT_HOST2 transmits "ICMPv6 Destination Unreachable with ESP3"

Possible Problems:

None.



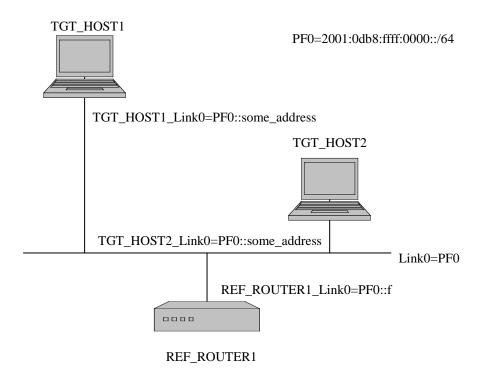
1.2. invoking Neighbor Unreachability Detection

Requirements:

- TGT_HOST1
 - ♦ Must support the application to send ICMPv6 Echo Request
- TGT_HOST2 (passive node)
 - ♦ Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply

Initialization:

Use following topology



Reboot TGT_HOST1 and TGT_HOST2 making sure it has cleared its neighbor cache.



Allow time for all devices on Link0 to perform Stateless Address Autoconfiguration and Duplicate Address Detection.

Set NUT's SAD and SPD as following:

(passive node TGT_HOST1 transport TGT_HOST2	e)
HOST1_SA1-0 spi=0x1000> HOST2_SA1-I HOST1_SA2-I < spi=0x2000 HOST2_SA2-0 HOST1_SA3-I < spi=0x3000 HOST2_SA3-0 HOST1_SA4-0 spi=0x4000> HOST2_SA4-I	ICMPv6 Echo Reply ICMPv6 Neighbor Solicitation

HOST1_SA1-O and HOST2_SA1-I

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

	HOST1_SA1-O	HOST2_SA1-I
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link0	
upper spec	ICMPv6 Echo Request	
direction	outbound inbound	
protocol	ESP	
mode	transport	



HOST1_SA2-I and HOST2_SA2-O

Security Association Database (SAD)

source address	TGT_HOST2_Link0
destination address	TGT_HOST1_Link0
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

Security Policy Database (SPD)

	HOST1_SA2-I	HOST2_SA2-O
source address	TGT_HOST2_Link0	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Echo Reply	
direction	inbound outbound	
protocol	ESP	
mode	transport	

HOST1_SA3-I and HOST2_SA3-O

Security Association Database (SAD)

source address	TGT_HOST2_Link0
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1sol
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1sol

	HOST1_SA3-I	HOST2_SA3-O
source address	TGT_HOST2_Link0	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Neighbor Solicitation	
direction	inbound outbound	
protocol	ESP	
mode	transport	



HOST1_SA4-O and HOST2_SA4-I

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link0
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2adv
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2adv

	HOST1_SA1-O	HOST2_SA1-I
source address	TGT_HOST1_Li	nk0
destination address	TGT_HOST2_Link0	
upper spec	ICMPv6 Neighbor Advertisement	
direction	outbound inbound	
protocol	ESP	
mode	transport	



Packets:

ICMPv6 Neighbor Solicitation (multicast)

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
		(solicited-node multicast address)
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address	TGT_HOST2_Link0
	Source link-layer address Option	

ICMPv6 Neighbor Advertisement

IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ICMPv6	Туре	136 (Neighbor Advertisement)
	S	true
	0	true
	Target Address	TGT_HOST2_Link0
	Target link-layer address Option	

ICMPv6 Echo Request with ESP1

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
ICMPv6	Type	128 (Echo Request)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
ICMPv6	Type	129 (Echo Reply)



ICMPv6 Neighbor Solicitation with ESP3

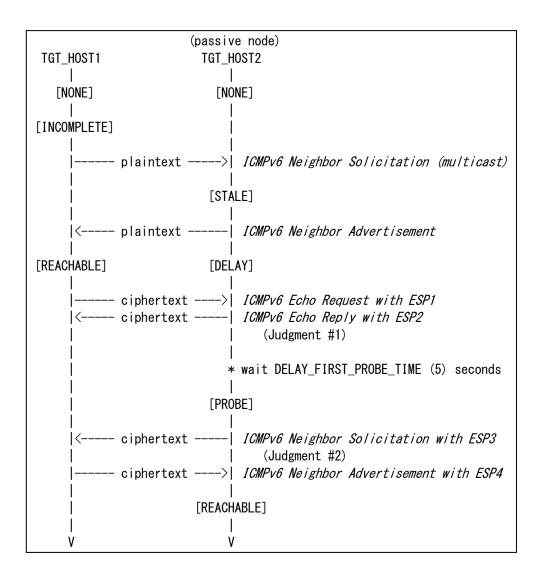
IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1sol
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1sol
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address	TGT_HOST1_Link0
	Source link-layer address Option	

ICMPv6 Neighbor Advertisement with ESP4

	8			
IPv6	Source Address	TGT_HOST1_Link0		
	Destination Address	TGT_HOST2_Link0		
ESP	SPI	0x4000		
	Algorithm	3DES-CBC		
	KEY	ipv6readylogo3des1to2adv		
	Authentication Algorithm	HMAC-SHA1		
	Authentication Key	ipv6readysha11to2adv		
ICMPv6	Type	136 (Neighbor Advertisement)		
	S	true		
	0	true		
	Target Address	TGT_HOST1_Link0		
	Target link-layer address Option			



Procedure:



- TGT_HOST1 sends "ICMPv6 Echo Request with ESP1" to TGT_HOST2
 * Address Resolution ("ICMPv6 Neighbor Solicitation (multicast)" and "ICMPv6 Neighbor Advertisement") is invoked
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Save the command log on TGT_HOST1
- Observe the packet transmitted by TGT_HOST2 for DELAY_FIRST_PROBE_TIME (5) seconds
- 5. Save the command log on TGT_HOST1



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMPv6 Echo Reply with ESP2"

Judgment #2

Step-4: TGT_HOST2 transmits "ICMPv6 Neighbor Solicitation with ESP3"

TGT_HOST1 responds to "ICMPv6 Neighbor Solicitation with ESP3" with
"ICMPv6 Neighbor Advertisement with ESP4"

Possible Problems:

None.



Appendix-C annex-5.3.8 for the passive node

This appendix describes alternative method to perform Test 5.3.8 on the passive node which doesn't have the application to send ICMPv6 Echo Request.

In these method, only TGT_HOST1 role can be the passive node.

Requirements:

- TGT_HOST1 (passive node)
 - ♦ Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply
 - ♦ Must respond to UDP packet toward the closed port with ICMPv6 Destination Unreachable (Port unreachable)
- TGT SGW1
 - ♦ No special requirements to perform this test for the passive node
- REF_HOST2
 - ♦ Must support the application to send ICMPv6 Echo Request
 - ♦ Must support the application to send UDP packet (e.g., DNS lookup client)

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
(passive node)
 TGT_HOST1 ======= tunnel ===== TGT_SGW1 ---- REF_HOST2
HOST1_SA1-I <---- spi=0x1000 ----- SGW1_SA1-0 ICMPv6 Echo Request
HOST1 SA2-0 ----- spi=0x2000 -----> SGW1 SA2-I ICMPv6 Echo Reply
HOST1_SA3-0 ----- spi=0x3000 -----> SGW1_SA3-I ICMPv6 Destination Unreachable
                                               (Port unreachable)
```



$HOST1_SA1\text{--}I \ and \ SGW1_SA1\text{--}O$

Security Association Database (SAD)

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3desstoereq
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1stoereq

	HOST1_SA1-I	SGW1_SA1-O
tunnel source address	TGT_SGW1_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	REF_HOST2_Link2	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Echo Request	
direction	inbound	outbound
protocol	ESP	
mode	tunnel	



$HOST1_SA2\text{-}O \ and \ SGW1_SA2\text{-}I$

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3desetosrep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1etosrep

	HOST1_SA2-O	SGW1_SA2-I
tunnel source address	TGT_HOST1_Link0	
tunnel destination address	TGT_SGW1_Link1	
source address	TGT_HOST1_Link0	
destination address	REF_HOST2_Link2	
upper spec	ICMPv6 Echo Re	ply
direction	outbound	inbound
protocol	ESP	
mode	tunnel	



$HOST1_SA3\text{-}O \ and \ SGW3_SA2\text{-}I$

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3desetosdst
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1etosdst

	HOST1_SA3-O	SGW1_SA3-I
tunnel source address	TGT_HOST1_Link0	
tunnel destination address	TGT_SGW1_Link1	
source address	TGT_HOST1_Link0	
destination address	REF_HOST2_Link2	
upper spec	ICMPv6 Destinati	ion Unreachable
direction	outbound	inbound
protocol	ESP	
mode	tunnel	



Packets:

ICMPv6 Echo Request

IPv6	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMPv6	Туре	128 (Echo Request)

ICMPv6 Echo Request with ESP1

	-	
IPv6	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3desstoereq
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1stoereq
IPv6	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	128 (Echo Request)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3desetosrep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosrep
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMPv6	Type	129 (Echo Reply)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMPv6	Туре	129 (Echo Reply)

UDP packet toward closed port

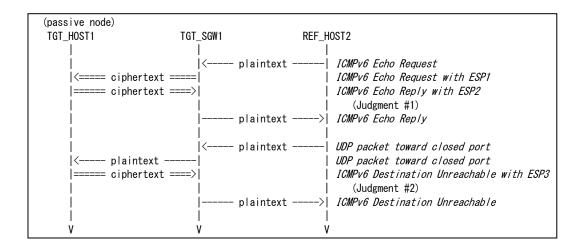
Ī	IPv6	Source Address	REF_HOST2_Link2
		Destination Address	TGT_HOST1_Link0
Γ	UDP	Source Port	Any unused port on REF_HOST2
		Destination Port	Any closed port on TGT_HOST1



ICMPv6 Destination Unreachable with ESP3

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3desetosdst
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosdst
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMPv6	Type	1 (Destination Unreachable)
	Code	4 (Port unreachable)

Procedure:



- 1. REF_HOST2 sends "ICMPv6 Echo Request" to TGT_HOST1
- 2. Observe the packet transmitted by TGT_HOST1
- 3. Save the command log on REF_HOST2
- 4. REF_HOST2 sends "UDP packet toward closed port" to TGT_HOST1
- 5. Observe the packet transmitted by TGT_HOST1
- 6. Save the command log on REF_HOST2



Judgment:

Judgment #1

Step-2: TGT_HOST1 transmits "ICMPv6 Echo Reply with ESP2"

Judgment #2

Step-5: TGT_HOST1 transmits "ICMPv6 Destination Unreachable with ESP3"

Possible Problems:

None.



Appendix-D annex-5.4.8 for the passive node

This appendix describes alternative methods to perform Test 5.4.8 on the passive node which doesn't have the application to send ICMPv6 Echo Request.

In these method, only TGT_HOST2 role can be the passive node. If TGT_HOST1 is the passive node, switch the role such that TGT_HOST2 is the passive node.



1.1.using UDP application to invoke ICMPv6 Destination

Unreachable (Port unreachable)

Requirements:

- ➤ TGT_HOST1
 - ♦ Must support the application to send ICMPv6 Echo Request
 - ♦ Must support the application to send UDP packet (e.g., DNS lookup client)
- ➤ TGT_HOST2 (passive node)
 - ♦ Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply
 - ♦ Must respond to UDP packet toward the closed port with ICMPv6 Destination Unreachable (Port unreachable)

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
(passive node)

TGT_HOST1 ======== tunnel ======= TGT_HOST2

HOST1_SA1-0 ----- spi=0x1000 -----> HOST2_SA1-I ICMPv6 Echo Request
HOST1_SA2-I <---- spi=0x2000 ------ HOST2_SA2-0 ICMPv6 Echo Reply
HOST1_SA3-I <---- spi=0x3000 ------ HOST2_SA3-0 ICMPv6 Destination Unreachable (Port unreachable)
```



$HOST1_SA1\text{-O and }HOST2_SA1\text{-I}$

Security Association Database (SAD)

TGT_HOST1_Link0	
TGT_HOST2_Link1	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3des1to2req	
HMAC-SHA1	
ipv6readysha11to2req	

	HOST1_SA1-O	HOST2_SA1-I
tunnel source address	TGT_HOST1_Link0	
tunnel destination address	TGT_HOST2_Link1	
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link1	
upper spec	ICMPv6 Echo Request	
direction	outbound inbound	
protocol	ESP	
mode	transport	



HOST1_SA2-I and HOST2_SA2-O

Security Association Database (SAD)

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3des2to1rep	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha12to1rep	

	HOST1_SA2-I	HOST2_SA2-O
tunnel source address	TGT_HOST2_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Echo Reply	
direction	inbound outbound	
protocol	ESP	
mode	transport	



HOST1_SA3-I and HOST2_SA3-O

Security Association Database (SAD)

source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
SPI	0x3000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3des2to1dst	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readysha12to1dst	

	HOST1_SA3-I	HOST2_SA3-O
tunnel source address	TGT_HOST2_Link1	
tunnel destination address	TGT_HOST1_Link0	
source address	TGT_HOST2_Link1	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Destination Unreachable	
direction	inbound outbound	
protocol	ESP	
mode	transport	



Packets:

ICMPv6 Echo Request with ESP1

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMPv6	Type	128 (Echo Request)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	129 (Echo Reply)

UDP packet toward closed port

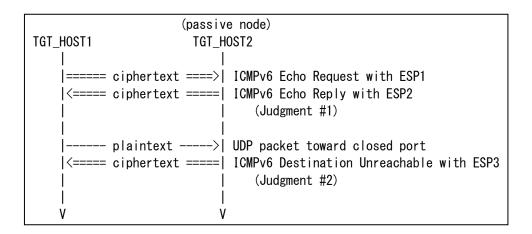
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
UDP	Source Port	Any unused port on TGT_HOST1
	Destination Port	Any closed port on TGT_HOST2

ICMPv6 Destination Unreachable with ESP3

IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1dst
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1dst
IPv6	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	1 (Destination Unreachable)
	Code	4 (Port unreachable)



Procedure:



- 1. TGT_HOST1 sends "ICMPv6 Echo Request with ESP1" to TGT_HOST2
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Save the command log on TGT_HOST1
- 4. TGT_HOST1 sends "UDP packet toward closed port" to TGT_HOST2
- 5. Observe the packet transmitted by TGT_HOST2
- 6. Save the command log on TGT_HOST1

Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMPv6 Echo Reply with ESP2"

Judgment #2

Step-5: TGT_HOST2 transmits "ICMPv6 Destination Unreachable with ESP3"

Possible Problems:

None.



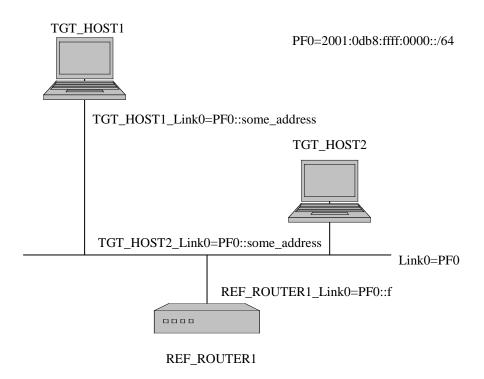
1.2. invoking Neighbor Unreachability Detection

Requirements:

- TGT_HOST1
 - ♦ Must support the application to send ICMPv6 Echo Request
- TGT_HOST2 (passive node)
 - ♦ Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply

Initialization:

Use following topology



Reboot TGT_HOST1 and TGT_HOST2 making sure it has cleared its neighbor cache.



Allow time for all devices on Link0 to perform Stateless Address Autoconfiguration and Duplicate Address Detection.

Set NUT's SAD and SPD as following:

(passive node TGT_HOST1 ======= tunnel ====== TGT_HOST2	e)
HOST1_SA1-0 spi=0x1000> HOST2_SA1-I HOST1_SA2-I < spi=0x2000 HOST2_SA2-0 HOST1_SA3-I < spi=0x3000 HOST2_SA3-0 HOST1_SA4-0 spi=0x4000> HOST2_SA4-I	ICMPv6 Echo Reply ICMPv6 Neighbor Solicitation

HOST1_SA1-O and HOST2_SA1-I

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

	HOST1_SA1-O	_
tunnel source address	TGT_HOST1_Li	nk0
tunnel destination address	TGT_HOST2_Li	nk0
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link0	
upper spec	ICMPv6 Echo Request	
direction	outbound inbound	
protocol	ESP	
mode	transport	



HOST1_SA2-I and HOST2_SA2-O

Security Association Database (SAD)

source address	TGT_HOST2_Link0
destination address	TGT_HOST1_Link0
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1rep

	HOST1_SA2-I	HOST2_SA2-O
tunnel source address	TGT_HOST2_I	ink0
tunnel destination address	TGT_HOST1_I	Link()
source address	TGT_HOST2_Link0	
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Echo Reply	
direction	inbound outbound	
protocol	ESP	
mode	transport	



HOST1_SA3-I and HOST2_SA3-O

Security Association Database (SAD)

source address	TGT_HOST2_Link0
destination address	TGT_HOST1_Link0
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1sol
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1sol

	HOST1_SA3-I	HOST2_SA3-O
tunnel source address	TGT_HOST2_I	ink0
tunnel destination address	TGT_HOST1_I	Link()
source address	TGT_HOST2_I	Link()
destination address	TGT_HOST1_Link0	
upper spec	ICMPv6 Neighbor Solicitation	
direction	inbound outbound	
protocol	ESP	
mode	transport	



HOST1_SA4-O and HOST2_SA4-I

Security Association Database (SAD)

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link0
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2adv
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2adv

	HOST1_SA1-O	HOST2_SA1-I
tunnel source address	TGT_HOST1_Li	nk0
tunnel destination address	TGT_HOST2_Li	nk0
source address	TGT_HOST1_Link0	
destination address	TGT_HOST2_Link0	
upper spec	ICMPv6 Neighbor Advertisement	
direction	outbound inbound	
protocol	ESP	
mode	transport	



Packets:

ICMPv6 Neighbor Solicitation (multicast)

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
		(solicited-node multicast address)
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address	TGT_HOST2_Link0
	Source link-layer address Option	

ICMPv6 Neighbor Advertisement

IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	136 (Neighbor Advertisement)
	S	true
	0	true
	Target Address	TGT_HOST2_Link0
	Target link-layer address Option	

ICMPv6 Echo Request with ESP1

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2req
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
ICMPv6	Type	128 (Echo Request)

ICMPv6 Echo Reply with ESP2

IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1rep
IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	129 (Echo Reply)



ICMPv6 Neighbor Solicitation with ESP3

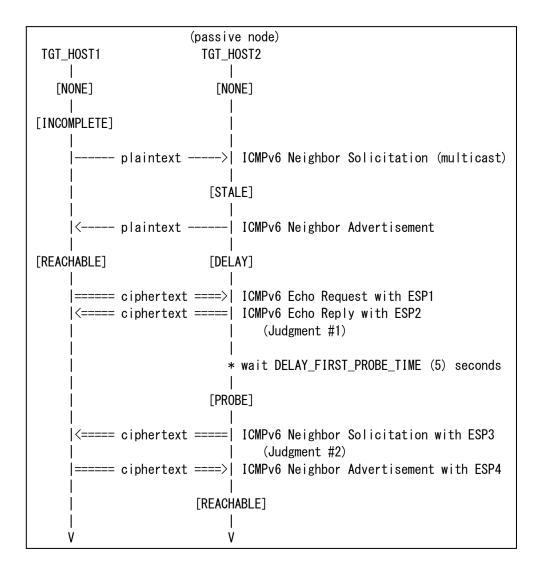
IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1sol
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1sol
IPv6	Source Address	TGT_HOST2_Link0
	Destination Address	TGT_HOST1_Link0
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address	TGT_HOST1_Link0
	Source link-layer address Option	

ICMPv6 Neighbor Advertisement with ESP4

IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des1to2adv
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2adv
IPv6	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link0
ICMPv6	Type	136 (Neighbor Advertisement)
	S	true
	0	true
	Target Address	TGT_HOST1_Link0
	Target link-layer address Option	



Procedure:



- TGT_HOST1 sends "ICMPv6 Echo Request with ESP1" to TGT_HOST2
 * Address Resolution ("ICMPv6 Neighbor Solicitation (multicast)" and "ICMPv6 Neighbor Advertisement") is invoked
- 2. Observe the packet transmitted by TGT_HOST2
- 3. Save the command log on TGT_HOST1
- 4. Observe the packet transmitted by TGT_HOST2 for DELAY_FIRST_PROBE_TIME (5) seconds
- 5. Save the command log on TGT_HOST1



Judgment:

Judgment #1

Step-2: TGT_HOST2 transmits "ICMPv6 Echo Reply with ESP2"

Judgment #2

Step-4: TGT_HOST2 transmits "ICMPv6 Neighbor Solicitation with ESP3"

TGT_HOST1 responds to "ICMPv6 Neighbor Solicitation with ESP3" with
"ICMPv6 Neighbor Advertisement with ESP4"

Possible Problems:

None.



All Rights Reserved. Copyright (C) 2004
Yokogawa Electric Corporation
IPv6 Forum

No part of this documentation may be reproduced for any purpose without prior permission.