



# **MODIFICATION RECORD**

Version 1.9.2	February 03, 2010
	<ul> <li>Corrected pre-shared key at subsection 5.1.5</li> </ul>
	<ul> <li>Corrected packet format of dummy packet at subsection 6.1.7</li> <li>Clarified relationship between steps in procedure and</li> </ul>
Varaion 1 0 1	judgment at all subsections.
Version 1.9.1	<ul> <li>January 07, 2009</li> <li>Support the passive node which doesn't have ping6 application (as Possible Problems in Section 5.1.2)</li> </ul>
Version 1.9.0	December 09, 2008
	<ul> <li>Support RFC 4312 (The Camellia Cipher Algorithm and Its Use With IPsec) (Section 5.2.7, 6.2.7)</li> </ul>
	• Use IPv6 prefix defined in RFC 3849 for the documentation
Version 1.8.1	October 11, 2007
	• Remove ESN test cases (Section 5.1.12, 6.1.14)
Version 1.8.0	April 27, 2007
	• Support IPsec v3
Version 1.7.7	April 6, 2006
	<ul> <li>Correct 5.3.4 Category</li> </ul>
Version 1.7.6	December 22, 2005
	<ul> <li>Correct expected MTU value in ICMP Packet Too Big message for 6.1.5 Packet Too Big Forwarding.</li> </ul>
Version 1.7.5	September 20, 2005
	<ul> <li>Correct the maximum MTU value for 6.1.4 Packet Too Big Transmission.</li> </ul>
Version 1.7.4	June 13, 2005
	<ul> <li>Fix typos.</li> </ul>
Version 1.7.3	June 7, 2005
	<ul> <li>Removed test for Packet Too Big Forwarding (Known Original Host) for SGW.</li> </ul>
Version 1.7.2	April 20, 2005
	<ul> <li>Fix typos.</li> </ul>
Version 1.7.1	April 18, 2005
	<ul> <li>Change Security Policy for 5.3.2.</li> </ul>
Version 1.7	April 8, 2005
	<ul> <li>Add Sequence Number Increment Test.</li> </ul>
	Add ICMP Error Test.
Version 1.6	March 1, 2005
	• Change Keys

Add Select SPD test for tunnel mode



Version 1.5	November 26, 2004
	<ul> <li>Change packet description of 5.1.4</li> </ul>
Version 1.4	November 19, 2004
	<ul> <li>Change Host to End-Node,</li> </ul>
	<ul> <li>Default algorithms changed to (3DES-CBC, HMAC-SHA1) for</li> </ul>
	Architecture test.
	<ul> <li>Editorial fix</li> </ul>
Version 1.3	September 24, 2004
Version 1.2	September 22, 2004
Version 1.1	September 13, 2004
Version 1.0	September 8, 2004



# **ACKNOWLEDGEMENT**

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

# **Principle Author:**

• TAHI Project

### **Commentators:**

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



# **INTRODUCTION**

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

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

The IPv6 Logo Program consists of three phases:

#### Phase 1:

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

#### Phase 2:

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

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

### Phase 3:

Same as Phase 2 with IPsec mandated.



# REQUIREMENTS

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 two possibilities for equipment types, they are as follows:

### 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:**

A NUT is required to pass all of the ESP tests regardless the equipment type. 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 an End-Node, it must pass all the Transport mode tests. If the NUT



supports the Tunnel mode, it also must pass all the Tunnel mode tests. (i.e., Tunnel mode is ADVANCED functionality for End-Node)

SGW:

If the NUT is a SGW, it must pass all the Tunnel mode tests.

### **Encryption Algorithm:**

IPv6 Logo Committee had defined 2 encryption algorithm categories: BASE ALGORITHM and ADVANCED ALGORITHM. All NUTs must pass the BASE ALGORITHM tests to obtain an IPsec Logo. A NUT which supports algorithms listed as ADVANCED ALGORITHM, must pass all 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

## **Category:**

All NUTs are required to support BASIC. ADVANCED is required for all NUTs which support ADVANCED encryption and/or authentication algorithms. Each test description contains a Category section which lists the requirements to satisfy the test.



# **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.



# TABLE OF CONTENTS

M	ODIFIC	ATION RECORD	1
A	CKNOW	LEDGEMENT	3
IN	TRODU	CTION	4
RI	EQUIRE	MENTS	5
RI	EFEREN	ICES	8
TA	ABLE OI	F CONTENTS	9
1.	Test D	etails	12
2.	Test T	opology	14
	For End	-Node: Transport and Tunnel Mode with End-Node Test	14
	For End	-Node: Tunnel Mode with SGW Test	15
	For SGV	V: Tunnel Mode with End-Node Test	16
	For SGV	V: Tunnel Mode Test	17
3.	Descri	ption	19
4.	Requi	red Tests	20
	For End	-Node:	21
	For SGV	V:	22
5.	End-N	Node Test	23
	5.1. A	rchitecture	23
	5.1.1.	Select SPD	24
	5.1.2.	Select SPD (ICMP Type)	29
	5.1.3.	Sequence Number Increment	34
	5.1.4.	Packet Too Big Reception	38
	5.1.5.	Receipt of No Next Header	43
	5.1.6.	Bypass Policy	48
	5.1.7.	Discard Policy	53
	5.1.8.	Transport Mode Padding	58
	5.1.9.	Transport Mode TFC Padding	62
	5.1.10	Non-Registered SPI	66



	5.1.11.	1CV	/0
5	.2. A	lgorithm Test	74
	5.2.1.	Transport Mode ESP=3DES-CBC HMAC-SHA1	75
	5.2.2.	Transport Mode ESP=3DES-CBC AES-XCBC	79
	5.2.3.	Transport Mode ESP=3DES-CBC NULL	83
	5.2.4.	Transport Mode ESP=AES-CBC (128-bit) HMAC-SHA1	87
	5.2.5.	Transport Mode ESP= AES-CTR HMAC-SHA1	91
	5.2.6.	Transport Mode ESP=NULL HMAC-SHA1	95
	5.2.7.	Transport Mode ESP=CAMELLIA-CBC (128-bit) HMAC-SHA1	99
5	.3. T	unnel Mode	103
	5.3.1.	Tunnel Mode with End-Node	103
	5.3.2.	Tunnel Mode with SGW	107
	5.3.3.	Select SPD for 2 Hosts behind 1 SGW	.111
	5.3.4.	Tunnel Mode Padding	.117
	5.3.5.	Tunnel Mode TFC Padding	122
			100
6.	SGW	Test	126
		rchitecture	
	.1. A		126
	.1. A	rchitecture	126 127
	<b>.1. A</b> 6.1.1.	Select SPD (ICMP Type)	126 127 134
	6.1.1. 6.1.2. 6.1.3.	Select SPD (ICMP Type)	126 127 134 141
	6.1.1. 6.1.2. 6.1.3. 6.1.4.	Select SPD (ICMP Type)	126 127 134 141 148
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5.	Select SPD	126 127 134 141 148 152
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6.	Select SPD	126 127 134 141 148 152
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7.	Select SPD	126 127 134 141 148 152 157
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8.	Select SPD	126 127 134 141 148 152 157 163 168
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8.	Select SPD Select SPD (ICMP Type) Select SPD for 2 Hosts behind 1 SGW Sequence Number Increment Packet Too Big Transmission Packet Too Big Forwarding (Unknown Original Host) Receipt of No Next Header Bypass Policy Discard Policy	126 127 134 141 148 152 157 163 168
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8.	Select SPD	126 127 134 141 148 152 157 163 168 173
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8. 6.1.9.	Select SPD	126 127 134 141 148 152 157 163 168 173 178
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8. 6.1.9. 6.1.10.	Select SPD	126 127 134 141 148 152 157 163 168 173 178 183
	6.1.1. 6.1.2. 6.1.3. 6.1.4. 6.1.5. 6.1.6. 6.1.7. 6.1.8. 6.1.9. 6.1.10. 6.1.11.	Select SPD	126 127 134 141 148 152 157 163 168 173 178 183 187



<b>6.2.</b> A	Algorithm Test	. 199
6.2.1.	Tunnel Mode ESP=3DES-CBC HMAC-SHA1	. 200
6.2.2.	Tunnel Mode ESP=3DES-CBC AES-XCBC	. 204
6.2.3.	Tunnel Mode ESP=3DES-CBC NULL	. 208
6.2.4.	Tunnel Mode ESP=AES-CBC (128-bit) HMAC-SHA1	. 212
6.2.5.	Tunnel Mode ESP=AES-CTR HMAC-SHA1	. 216
6.2.6.	Tunnel Mode ESP=NULL HMAC-SHA1	. 220
6.2.7.	Tunnel Mode ESP= CAMELLIA-CBC (128-bit) HMAC-SHA1	. 224
Appendix-	-A annex-5.1.2 for the passive node	. 228
1.1. v	using UDP application to invoke ICMPv6 Destination Unreachable	(Port
unreacha	able)	. 229
1.2. i	nvoking Neighbor Unreachability Detection	. 234



# 1. Test Details

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

### **Terminology:**

TN: Tester Node

NUT: Node Under Test (Target Implementation)

SGW : Security Gateway

### **Required Application:**

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

## **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: Transport and Tunnel Mode with End-Node Test

- 1. Set global address to NUT by RA (NUT\_Link0)
- 2. Set MTU to NUT by RA (MTU value is 1500 for Link0)
- 3. Make IPsec transport mode between NUT and HOST1 and HOST2

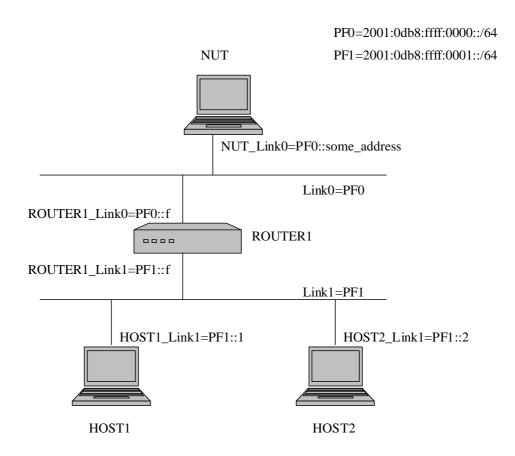


Fig. 1 Topology for End-Node: Transport and Tunnel mode with End-Node



## For End-Node: Tunnel Mode with SGW Test

- 1. Set global address to NUT by RA (NUT\_Link0)
- 2. Set MTU to NUT by RA (MTU value is 1500 for Link0)
- 3. Make IPsec tunnel mode between NUT and SGW1.

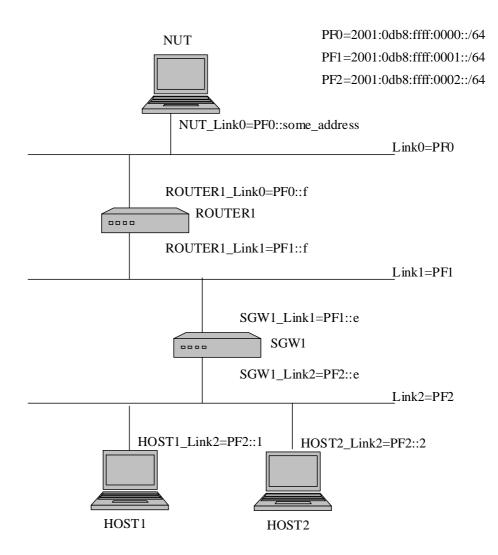


Fig. 2 Topology for End-Node: Tunnel mode with SGW



### For SGW: Tunnel Mode with End-Node Test

- 1. Set global address to NUT manually (NUT\_Link0, NUT\_Link1)
- 2. Set routing table to NUT manually (ROUTER1\_Link1 for Link2)
- 3. Set MTU to NUT manually for Link0 and Link1 (MTU value is 1500 for Link0 and Link1)
- 4. Make IPsec tunnel mode between NUT and HOST2.

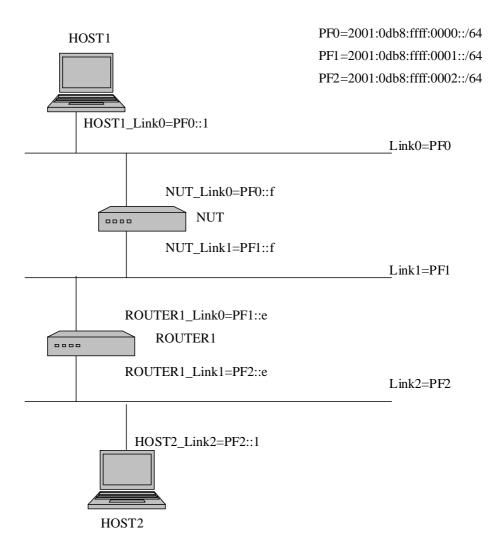


Fig. 3 Topology for SGW: Tunnel mode with End-Node



## **For SGW: Tunnel Mode Test**

- 1. Set global address to NUT manually (NUT\_Link0, NUT\_Link1)
- 2. Set routing table to NUT manually (ROUTER1\_Link1 for Link2, Link3 and Link4)
- 3. Set MTU to NUT manually for Link0 and Link1 (MTU value is 1500 for Link0 and Link1)
- 4. Make IPsec tunnel mode between NUT and SGW1 and SGW2



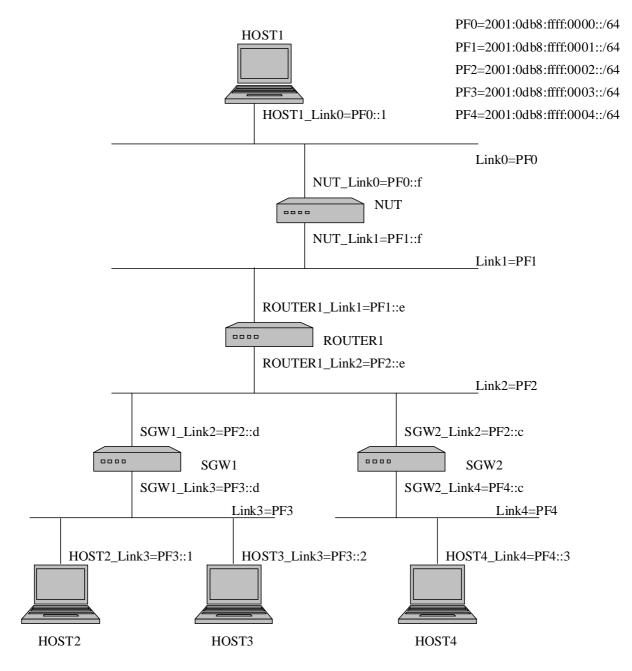


Fig. 4 Topology for SGW: Tunnel mode with SGW



# 3. Description

Each test specification consists of following parts.

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

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

**Category:** The Category shows what classification of device must satisfy the test.

**References:** The References section contains some parts of specification related to the tests. It

also shows the document names and section numbers.

**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.

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

**Results:** description of Judgment, the NUT passes the test.

**Possible** This section contains a description of known issues with the test procedure, which

**Problems:** may affect test results in certain situations.



# 4. Required Tests

The following table lists which tests a device is required to pass based on category.



# For End-Node:

Test Title	Category	Note
Select SPD	BASIC	
Select SPD (ICMP Type)	ADVANCED	IPsec v3 Must be tested by ICMP
Sequence Number Increment	BASIC	
Packet Too Big Reception	BASIC	
Receipt of No Next Header	ADVANCED	IPsec v3
Bypass Policy	ADVANCED	Either of Bypass or Discard
Discard Policy	ADVANCED	Policy is required
Transport Mode Padding	BASIC	
Transport Mode TFC Padding	ADVANCED	IPsec v3 Must be tested by UDP
Non-Registered SPI	BASIC	
ICV	BASIC	
Transport Mode ESP=3DES-CBC HMAC-SHA1	BASIC	
Transport Mode ESP=3DES-CBC AES-XCBC	ADVANCED	
Transport Mode ESP=3DES-CBC NULL	ADVANCED	
Transport Mode ESP=AES-CBC (128-bit) HMAC-SHA1	ADVANCED	
Transport Mode ESP=AES-CTR HMAC-SHA1	ADVANCED	IPsec v3
Transport Mode ESP=NULL HMAC-SHA1	ADVANCED	
Transport Mode ESP=CAMELLIA-CBC (128-bit) HMAC-SHA1	ADVANCED	
Tunnel Mode with End-Node	ADVANCED	
Tunnel Mode with SGW	ADVANCED	
Select SPD for 2 Hosts behind 1 SGW	ADVANCED	
Tunnel Mode Padding	ADVANCED	
Tunnel Mode TFC Padding	ADVANCED	IPsec v3



# For SGW:

Test Title	Category	Note
Select SPD	BASIC	
Select SPD (ICMP Type)	ADVANCED	IPsec v3
Select SFD (Tomir Type)	ADVANCED	Must be tested by ICMP
Select SPD for 2 Hosts behind 1 SGW	BASIC	
Sequence Number Increment	BASIC	
Packet Too Big Transmission	BASIC	
Packet Too Big Forwarding(Unknown Original Host)	BASIC	
Receipt of No Next Header	ADVANCED	IPsec v3
Bypass Policy	ADVANCED	Either of Bypass or Discard Policy
Discard Policy	ADVANCED	is required
Tunnel Mode Padding	BASIC	
Tunnel Mode TFC Padding	ADVANCED	IPsec v3
Non-Registered SPI	BASIC	
ICV	BASIC	
Tunnel Mode with End-Node	BASIC	
Tunnel Mode ESP=3DES-CBC HMAC-SHA1	BASIC	
Tunnel Mode ESP=3DES-CBC AES-XCBC	ADVANCED	
Tunnel Mode ESP=3DES-CBC NULL	ADVANCED	
Tunnel Mode ESP=AES-CBC (128-bit) HMAC-SHA1	ADVANCED	
Tunnel Mode ESP=AES-CTR HMAC-SHA1	ADVANCED	IPsec v3
Tunnel Mode ESP=NULL HMAC-SHA1	ADVANCED	
Tunnel Mode ESP=CAMELLIA-CBC (128-bit) HMAC-SHA1	ADVANCED	



# 5. End-Node Test

This Chapter describes the test specification for End-Node. The test specification consists of 2 sections. One is regarding "IPsec Architecture" and another part is regarding "Encryption and Authentication Algorithms".

# 5.1. Architecture

### Scope:

Following tests focus on IPsec Architecture.

### Overview:

Tests in this section verify that a node properly process and transmit based on the Security Policy Database and Security Association Database.



## **5.1.1. Select SPD**

### Purpose:

Verify that a NUT (End-Node) selects appropriate SPD (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

### Category:

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

SGW : N/A

### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1_Link1		
	>	SA1-I
	<	SA1-0
HOST2 Link1		NUT
_	>	SA2-I
	<	



## Security Association Database (SAD) for SA1-I

Codd it y Modes i at i at a a a a a a a a a a a a a a a		
HOST1_Link1		
NUT_Link0		
0x1000		
transport		
ESP		
3DES-CBC		
ipv6readylogo3descbcin01		
HMAC-SHA1		
ipv6readylogsha1in01		

### Security Policy Database (SPD) for SA1-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



### Security Association Database (SAD) for SA2-I

HOST2_Link1	
NUT_Link0	
0x3000	
transport	
ESP	
3DES-CBC	
ipv6readylogo3descbcin02	
HMAC-SHA1	
ipv6readylogsha1in02	

### Security Policy Database (SPD) for SA2-I

source address	HOST2_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA2-0

source address	NUT_Link0
destination address	HOST2_Link1
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD) for SA2-0

source address	NUT_Link0
destination address	HOST2_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



### Packets:

## ICMP Echo Request with SA1's ESP

Tomi Zono nogace		
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

### ICMP Echo Reply with SA1's ESP

Tomi Lone Hopiy II	1 211 2111 2 221	
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Туре	129 (Echo Reply)

## ICMP Echo Request with SA2's ESP

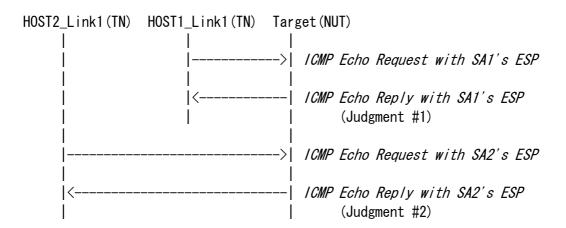
	11 1 21 21 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
IP Header	Source Address	HOST2_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply with SA2's ESP

IP Header	Source Address	NUT_Link0
	Destination Address	H0ST2_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMP	Type	129 (Echo Reply)



#### Procedure:



### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with SA1's ESP"
- 2. Observe the packet transmitted by NUT
- 3. Host2 sends "ICMP Echo Request with SA2's ESP"
- 4. Observe the packet transmitted by NUT

### Observable Results:

### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Reply with SA1's ESP".
Step-4 (Judgment #2):

NUT transmits "ICMP Echo Reply with SA2's ESP".

### Possible Problems:

None.



# **5.1.2. Select SPD (ICMP Type)**

### Purpose:

Verify that a NUT (End-Node) selects appropriate SPD (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

IPsec v3)

SGW : N/A

### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ----- NUT -----> SA1-I <----- SA1-0 -----> SA2-I <----- SA2-0



## Security Association Database (SAD) for SA1-I

COOCHIES NOODOTALTON DALABAGO (OND) TOT ONT T	
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

## Security Policy Database (SPD) for SA1-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	ICMPv6 Echo Request
direction	out
protocol	ESP
mode	transport



### Security Association Database (SAD) for SA2-I

source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin02
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in02

### Security Policy Database (SPD) for SA2-I

source address	HOST1_Link1
destination address	NUT_LinkO
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA2-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD) for SA2-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	ICMPv6 Echo Reply
direction	out
protocol	ESP
mode	transport



### Packets:

# ICMP Echo Request with SA1-I's ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

### ICMP Echo Reply with SA2-0's ESP

Tomi Lone Hopiy ii	7 6/1 6/12 6 6 26/	
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

## ICMP Echo Request with SA1-0's ESP

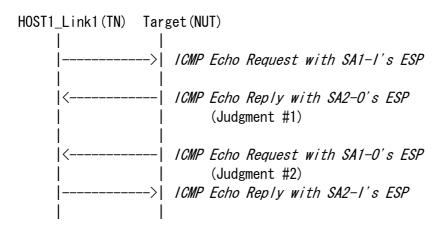
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply with SA2-I's ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMP	Type	129 (Echo Reply)



#### Procedure:



#### Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with SA1-I's ESP"
- 2. Observe the packet transmitted by NUT
- 3. NUT sends "ICMP Echo Request with SA1-0's ESP"
- 4. Observe the packet transmitted by NUT
- 5. HOST1 sends "ICMP Echo Reply with SA2-I's ESP"

#### Observable Results:

#### Part A:

```
Step-2 (Judgment #1):
   NUT transmits "/CMP Echo Reply with SA2-0's ESP".
Step-4 (Judgment #2):
   NUT transmits "/CMP Echo Request with SA1-0's ESP".
```

#### Possible Problems:

NUT 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-A Section 1.1)
- b) invoking Neighbor Unreachability Detection (see Appendix-A Section 1.2)



# **5.1.3. Sequence Number Increment**

### Purpose:

Verify that a NUT (End-Node) increases sequence number correctly, starting with 1. (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

### Category:

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

SGW : N/A

### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



### Security Association Database (SAD) for SA-I

•	·
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



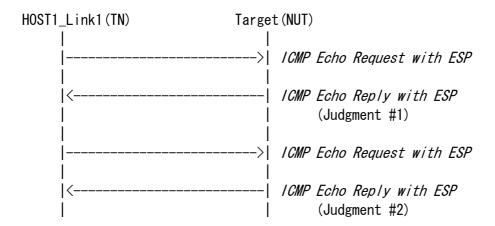
# ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1	
	Destination Address	NUT_Link0	
ESP	SPI	0x1000	
	Sequence	$1^{st} = 1, 2^{nd} = 2$	
	Algorithm	3DES-CBC	
	KEY	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
ICMP	Type	128 (Echo Request)	

# ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Sequence	$1^{st} = 1, 2^{nd} = 2$
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)





#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Request with ESP"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits an "ICMP Echo Reply with ESP" with an ESP Sequence Number of 1.

Step-4 (Judgment #2):

NUT transmits an "ICMP Echo Reply with ESP" with an ESP Sequence Number of 2.

#### Possible Problems:



# **5.1.4. Packet Too Big Reception**

## Purpose:

Verify that a NUT (End-Node) process the ICMP Error Message (Packet Too Big) correctly. (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

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

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1. Router1's interface to Link1 has an MTU value of 1280.

Set NUT's SAD and SPD as following:

HOST1_Link1		NUT
	>	SA-I
	<b>&lt;</b>	SA-0



## Security Association Database (SAD) for SA-I

order to the contract of bacasace (chb, to to the the		
source address HOST1_Link1		
destination address	NUT_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

,			
IP Header	Source Address	HOST1_Link1	
	Destination Address	NUT_Link0	
	Payload Length	1460	
ESP	SPI	0x1000	
	Algorithm	3DES-CBC	
	KEY	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
ICMP	Type	128 (Echo Request)	

## ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
	Payload Length	1460
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

## ICMP Error Message (Packet Too Big)

IP Header	Source Address	Router_Link1
	Destination Address	NUT_Link0
ICMP	Type	2 (Packet Too Big)
	MTU	1280
	Data	1232Byte of ICMP Echo Reply with
		ESP



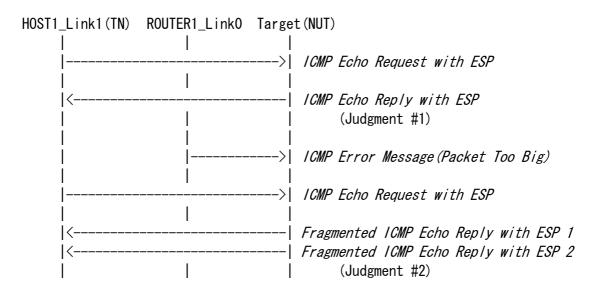
# Fragmented ICMP Echo Reply with ESP 1

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
	Payload Length	1240
Fragment	Offset	0
	More Flag	1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

# Fragmented ICMP Echo Reply with ESP 2

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
	Payload Length	236
Fragment	Offset	154
	More Flag	0
Data	Data	Rest of <i>ICMP Echo Reply with ESP</i>





#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT
- 3. ROUTER1 sends "ICMP Error Message (Packet Too Big)
- 4. HOST1 sends "ICMP Echo Request with ESP"
- 5. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

Step-5 (Judgment #2):

NUT transmits "Fragmented ICMP Echo Reply with ESP 1" and "Fragmented ICMP Echo Reply with ESP 2"

#### Possible Problems:



## 5.1.5. Receipt of No Next Header

## Purpose:

Verify that a NUT (End-Node) process the dummy packet (the protocol value 59) correctly. (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

IPsec v3)

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA1-I <------ SA1-0



## Security Association Database (SAD) for SA1-I

Total Ity necestation bacasacs (one, ion on i		
HOST1_Link1		
NUT_Link0		
0x1000		
transport		
ESP		
3DES-CBC		
ipv6readylogo3descbcin01		
HMAC-SHA1		
ipv6readylogsha1in01		

#### Security Policy Database (SPD) for SA1-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with SA1-I's ESP

	Tem Lette Hequeet With the Let		
IP Header	Source Address	HOST1_Link1	
	Destination Address	NUT_Link0	
ESP	SPI	0x1000	
	Algorithm	3DES-CBC	
	Key	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
ICMP	Type	128 (Echo Request)	

## ICMP Echo Reply with SA1-0's ESP

	Tomi Lone Hopry With Oth C C Lor		
IP Header	Source Address	NUT_Link0	
	Destination Address	HOST1_Link1	
ESP	SPI	0x2000	
	Algorithm	3DES-CBC	
	Key	ipv6readylogo3descbcout1	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1out1	
ICMP	Type	129 (Echo Reply)	

# No Next Header with SA1-I's ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Next Header	no next header (59)
Upper Layer	Data	empty



Part A (ADVANCED): No Next Header w/o TFC Padding

- 1. HOST1 sends "ICMP Echo Request with SA1-I's ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "No Next Header with SA1-O's ESP". The ESP sequence number must be incremented than the packet transmitted at step 1
- 4. HOST1 sends "ICMP Echo Request with SA1-0's ESP". The ESP sequence number must be incremented than the packet transmitted at step 3
- 5. Observe the packet transmitted by NUT

Part B (ADVANCED): No Next Header w/ TFC Padding

- 6. HOST1 sends "ICMP Echo Request with SA1-1's ESP"
- 7. Observe the packet transmitted by NUT
- 8. HOST1 sends "No Next Header with SA1-O's ESP". The ESP sequence number must be incremented than the packet transmitted at step 6. The data in upper layer consists of random bytes as the plaintext portion.
- 9. HOST1 sends "ICMP Echo Request with SA1-0's ESP". The ESP sequence number must be incremented than the packet transmitted at step 8
- 10. Observe the packet transmitted by NUT



## Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Reply with SA1-0's ESP".
Step-5 (Judgment #2):
NUT transmits "ICMP Echo Reply with SA1-0's ESP".

Part B:
Step-7 (Judgment #1):
NUT transmits "ICMP Echo Reply with SA1-0's ESP".
Step-10 (Judgment #2):
NUT transmits "ICMP Echo Reply with SA1-0's ESP".
```

#### Possible Problems:



## **5.1.6.** Bypass Policy

#### Purpose:

Verify that a NUT (End-Node) select bypass or discard policies

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Bypass Policy, regardless of explicitly or implicitly)

SGW : N/A

NOTE: NUT needs to pass at least either of "Bypass Policy" or "Discard Policy" tests.

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ----- NUT -----> SA-I



## Security Association Database (SAD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

## Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
	Payload Length	1460
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
	Payload Length	1460
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

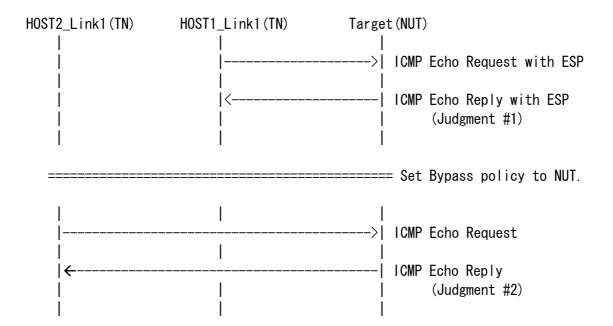
## ICMP Echo Request

IP Header	Source Address	H0ST2_Link1
	Destination Address	NUT_Link0
ICMP	Туре	128 (Echo Request)

## ICMP Echo Reply

IP Header	Source Address	NUT_Link0
	Destination Address	HOST2_Link1
ICMP	Type	129 (Echo Reply)





Part A (ADVANCED -- except Either of Bypass or Discard Policy is required):

- 1. Host1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT
- 3. Set Bypass policy for above ICMP Echo Request to NUT as following example
- 4. HOST1 sends "ICMP Echo Request"
- 5. Observe the packet transmitted by NUT

Example 1: Security Policy Database (SPD) for policy=Bypass

source address	H0ST2_Link1
destination address	NUT_Link0
upper spec	any
direction	in
policy	bypass (none)

Example 2: Security Policy Database (SPD) for policy=Bypass as default policy

source address	any
destination address	any
upper spec	any
direction	in
policy	bypass (none)



## Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "/CMP Echo Reply with ESP"
Step-5 (Judgment #2):
NUT transmits "/CMP Echo Reply"
```

## Possible Problems:



## **5.1.7. Discard Policy**

#### Purpose:

Verify that a NUT (End-Node) select bypass or discard policies

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Discard Policy, regardless of explicitly or implicitly)

SGW : N/A

NOTE: NUT need to pass at least either of "Bypass Policy" or "Discard Policy" tests.

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ----- NUT -----> SA-I



## Security Association Database (SAD) for SA-I

source address	HOST1_Link1
destination address NUT_LinkO	
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

## Security Association Database (SAD) for SA-0

source address	NUT_Link0	
destination address	HOST1_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key ipv6readylogsha1out1		

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
	Payload Length	1460
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

# ICMP Echo\_Reply\_with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
	Payload Length	1460
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

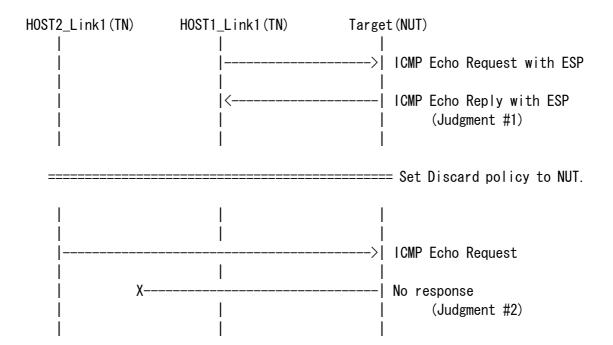
## ICMP Echo Request

IP Header	Source Address	H0ST2_Link1
	Destination Address	NUT_Link0
ICMP	Туре	128 (Echo Request)

# ICMP Echo Reply

IP Header	Source Address	NUT_Link0
	Destination Address	HOST2_Link1
ICMP	Type	129 (Echo Reply)





Part A (ADVANCED -- except Either of Bypass or Discard Policy is required):

- 1. Host1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT
- 3. Set Discard policy for above ICMP Echo Request to NUT as following example
- 4. HOST1 sends "ICMP Echo Request"
- 5. Observe the packet transmitted by NUT

Example 1: Security Policy Database (SPD) for policy=Discard

source address	HOST1_Link1	
destination address	NUT_Link0	
upper spec	any	
direction	in	
policy	discard	

Example 2: Security Policy Database (SPD) for policy=Discard as default policy

source address	any
destination address	any
upper spec	any
direction	in
policy	discard



## Observable Results:

Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Reply with ESP"
Step-5 (Judgment #2):
NUT does not transmit any packets.

## Possible Problems:



## **5.1.8. Transport Mode Padding**

## Purpose:

Verify that a NUT (End-Node) supports padding & padding byte handling (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

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

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



## Security Association Database (SAD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

## Security Association Database (SAD) for SA-0

coon to y the coot and the contract (cris) to the contract contract (cris) to the contract co	
source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP 1

Telli Zerre Regueet irreir zer r		
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
Authentication Algorithm		HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Padding	Sequential
	Padding Length	7
ICMP	Туре	128 (Echo Request)
	Data Length	7

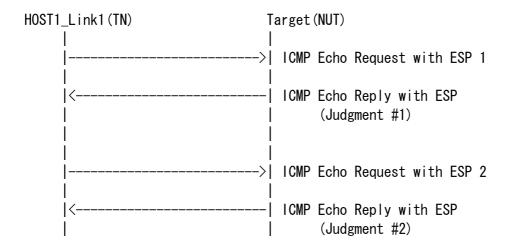
# ICMP Echo Request with ESP 2

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Padding	Sequential
	Padding Length	255
ICMP	Type	128 (Echo Request)
	Data Length	7

# ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
	Padding Length	7+8n (0 <= n <= 31)
ICMP	Type	129 (Echo Reply)
	Data Length	7





## Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP 1"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Request with ESP 2"
- 4. Observe the packet transmitted by NUT

## Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

Step-4 (Judgment #2):

NUT transmits "ICMP Echo Reply with ESP"

#### Possible Problems:



## 5.1.9. Transport Mode TFC Padding

## Purpose:

Verify that a NUT (End-Node) supports TFC Padding (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

IPsec v3)

SGW : N/A

#### References:

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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA1-I <------ SA1-0



## Security Association Database (SAD) for SA1-I

decartery housestation bacasage (chb) for our i		
source address	HOST1_Link1	
destination address	NUT_Link0	
SPI	0x1000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

## Security Policy Database (SPD) for SA1-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA1-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



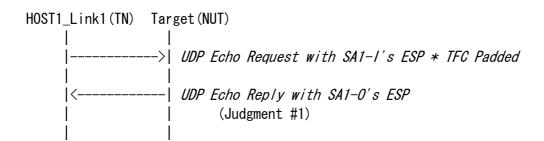
# UDP Echo Request with SA1-I's ESP \* TFC Padded

er zene negatet mien en rie zen in er aande		
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
UDP	Source Port	10000
	Destination Port	7 (echo)

## UDP Echo Reply with SA1-0's ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
UDP	Source Port	7 (echo)
	Destination Port	10000





## Part A (ADVANCED):

- 1. HOST1 sends "UDP Echo Request with SA1-I's ESP \* TFC Padded"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "UDP Echo Reply with SA1-0's ESP".

## Possible Problems:



# 5.1.10. Non-Registered SPI

## Purpose:

Verify that a NUT (End-Node) can behave when No valid Security Association is configured.

## Category:

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

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

## Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

66



## Security Association Database (SAD) for SA-I

·	
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

## Security Association Database (SAD) for SA-0

coon reg more acres. Datamate (crib) res est e		
source address	NUT_Link0	
destination address	HOST1_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



## ICMP Echo Request with ESP 1

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

## ICMP Echo Reply with ESP 1

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

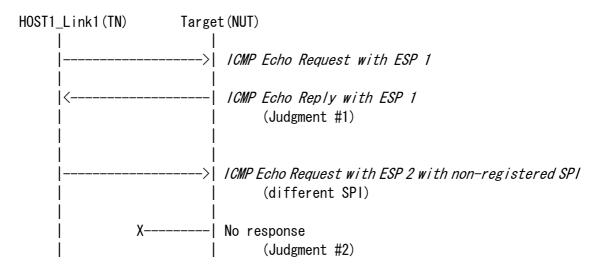
## ICMP Echo Request with ESP 2 with non-registered SPI

Tomi Lone Regade With Lor 2 With hon regretered of t		
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x9000 (Different from SA-I's
		SPD)
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ICMP	Type	129 (Echo Reply)





#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP 1"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Request with ESP 2" (different SPI)
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Reply with ESP 1"
Step-4 (Judgment #2):
 NUT does not transmit any packets.

#### Possible Problems:



## 5.1.11. ICV

## Purpose:

Verify that a NUT (End-Node) can detect the modification by examining the ICV (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

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

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



## Security Association Database (SAD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

## Security Association Database (SAD) for SA-0

cocal its, horsestation bacasact (chb) its one		
source address	NUT_Link0	
destination address	HOST1_Link1	
SPI	0x2000	
mode	transport	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP 1

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Sequence number	1
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)
	Data	"EchoData"

# ICMP Echo Reply with ESP 1

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Туре	129 (Echo Reply)
	Data	"EchoData"

# ICMP Echo Request with ESP 2

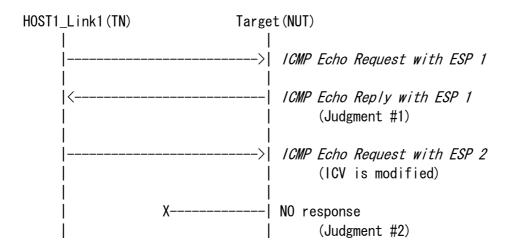
TOMI LOTTO HOGACOL	WITCH LOT L	
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Sequence number	2
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	ICV	aaaaaaaaaaaaaaaa
ICMP	Type	128 (Echo Request)
	Data	"cracked"

# ICMP Echo Reply

	. ,		
IP Header	Source Address	NUT_Link0	
	Destination Address	HOST1_Link1	
ICMP	Type	129 (Echo Reply)	



#### Procedure:



#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP 1"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Request with ESP 2" (ICV is modified)
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP 1"
Step-4 (Judgment #2):

NUT does not transmit any packets.

#### Possible Problems:



# **5.2.** Algorithm Test

## Scope:

Following tests focus on Encryption and Authentication Algorithms.

#### Overview:

Tests in this section verify that the NUT properly decrypt the received packet s and encrypts the transmitting packets using Encryption algorithms specified in the SAD.

And they verify that the NUT properly processes the authentication algorithms specified in the SAD.



# 5.2.1. Transport Mode ESP=3DES-CBC HMAC-SHA1

Purpose:	Ρι	ırpo	se
----------	----	------	----

End-Node transport mode, 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]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



•	·
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

#### ICMP Echo Reply with ESP

Tomi Lone Hopry Wi	CIT LOT	
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target(NUT)
	>  <i>ICMP Echo Request with ESF</i>
<	ICMP Echo Reply with ESP
I	(Judgment #1)

#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "/CMP Echo Reply with ESP"

## Possible Problems:





# 5.2.2. Transport Mode ESP=3DES-CBC AES-XCBC

#### Purpose:

End-Node transport mode, ESP=3DES-CBC AES-XCBC

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

AES-XCBC as an authentication algorithm)

SGW : N/A

#### References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ----- NUT -----> SA-I <----- SA-0



source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesxin01

# Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesxout1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



## ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	AES-XCBC-MAC-96
	Authentication Key	ipv6readaesxin01
ICMP	Type	128 (Echo Request)

#### ICMP Echo Reply with ESP

Tomi Lone Hopry Wi	CIT LOT	
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	AES-XCBC-MAC-96
	Authentication Key	ipv6readaesxout1
ICMP	Type	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target(NUT)
	>  <i>ICMP Echo Request with ESF</i>
<	ICMP Echo Reply with ESP
I	(Judgment #1)

#### Part A (ADVANCED)

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

#### Possible Problems:





# **5.2.3. Transport Mode ESP=3DES-CBC NULL**

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

End-Node transport mode, ESP=3DES-CBC NULL

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

NULL as an authentication algorithm)

SGW : N/A

#### References:

- [RFC2410]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1_Link1		
	>	SA-I
	<b>&lt;</b>	SA-0

83



source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	NULL
ESP authentication key	

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	NULL
ESP authentication key	

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



## ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	NULL
	Authentication Key	
ICMP	Type	128 (Echo Request)

#### ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	H0ST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	NULL
	Authentication Key	
ICMP	Type	129 (Echo Reply)

#### Procedure:

arget(NUT)	Target	Γ1_Link1(TN)	HOST1_
>  <i>ICMP Echo Request with ES</i>			
<i>ICMP Echo Reply with ESP</i>		<	
(Judgment #1)			

#### Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

## Possible Problems:





# 5.2.4. Transport Mode ESP=AES-CBC (128-bit) HMAC-SHA1

#### Purpose:

End-Node transport mode, ESP=AES-CBC (128-bit) HMAC-SHA1

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

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

SGW : N/A

#### References:

- [RFC2404]
- [RFC3602]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



<u> </u>	·
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-0

(c/.2)	
source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



## ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

#### ICMP Echo Reply with ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target(NUT)
	>  <i>ICMP Echo Request with ESF</i>
<	ICMP Echo Reply with ESP
I	(Judgment #1)

#### Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

## Possible Problems:





# 5.2.5. Transport Mode ESP= AES-CTR HMAC-SHA1

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

End-Node transport mode, ESP= AES-CTR HMAC-SHA1

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

AES-CTR as an encryption algorithm)

SGW : N/A

#### References:

- [RFC3686]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



occurred Macadada (M.B., Tot. C.).	
HOST1_Link1	
NUT_Link0	
0x1000	
transport	
ESP	
AES-CTR	
ipv6readylogaescin01	
HMAC-SHA1	
ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogaescout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogaescin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Туре	128 (Echo Request)

#### ICMP Echo Reply with ESP

TOME LOTTO HOPTY		
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogaescout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Туре	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target(NUT)
	>  <i>ICMP Echo Request with ESF</i>
<	ICMP Echo Reply with ESP
I	(Judgment #1)

## Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

#### Possible Problems:





# 5.2.6. Transport Mode ESP=NULL HMAC-SHA1

<b>Purpose</b>	:	
i di podo	•	

End-Node transport mode, ESP=NULL HMAC-SHA1

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

NULL as an encryption algorithm)

SGW : N/A

#### References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ----- NUT ----> SA-I <----- SA-0



Total Tel Moderation Database (OND) Tel ON T	
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP algorithm key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

## Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-O

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP algorithm key	
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	transport



## ICMP Echo Request with ESP

IP Header Source Address		HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Type	128 (Echo Request)

#### ICMP Echo Reply with ESP

Tomi Lone Nobity With Lon		
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Туре	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target (NUT)
 	 >  <i>ICMP Echo Request with ESF</i>
	<i>ICMP Echo Reply with ESP</i>   (Judgment #1)

#### Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

#### Possible Problems:





# 5.2.7. Transport Mode ESP=CAMELLIA-CBC (128-bit) HMAC-SHA1

Dur	pose	
rui	POSE	•

End-Node transport mode, ESP=CAMELLIA-CBC (128-bit) HMAC-SHA1

## Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

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

SGW : N/A

#### References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4312]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

HOST1\_Link1 ------ NUT -----> SA-I <------ SA-0



11	HOOTA I ' I A
source address	HOST1_Link1
Destination address	NUT_Link0
SPI	0x1000
Mode	transport
Protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipvcamelliacin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

source address	HOST1_Link1
destination address	NUT_LinkO
upper spec	Any
direction	In
protocol	ESP
mode	transport

# Security Association Database (SAD) for SA-0

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipvcamelliacout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	Any
direction	Out
protocol	ESP
mode	transport



# ICMP Echo Request with ESP

IP Header Source Address		HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipvcamelliacin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply with ESP

Tomi Lone Nobity With Lon		
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipvcamelliacout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
ICMP	Type	129 (Echo Reply)

#### Procedure:

HOST1_Link1(TN)	Target (NUT)
 	 >  <i>ICMP Echo Request with ESF</i>
	<i>ICMP Echo Reply with ESP</i>   (Judgment #1)

#### Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Reply with ESP"

#### Possible Problems:





# 5.3. Tunnel Mode

#### 5.3.1. Tunnel Mode with End-Node

#### Purpose:

Verify that a NUT (End-Node) can build IPsec tunnel mode with End-Node correctly. (End-Node tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Tunnel Mode)

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



•	·
source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

tunnel source address	HOST1_Link1
tunnel destination address	NUT_Link0
source address	HOST1_Link1
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

#### Security Association Database (SAD) for SA-0

documents house action bacasace (one) for one		
source address	NUT_Link0	
destination address	HOST1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

tunnel source address	NUT_Link0
tunnel destination address	HOST1_Link1
source address	NUT_Link0
destination address	HOST1_Link1
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP tunnel

IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ICMP	Type	129 (Echo Reply)



#### Procedure:

HOST1_Link1(TN)	Target (NUT)	
	 >  ICMP Echo Request within ESP tunne	<del>?</del> /
  < 	   <i>ICMP Echo Reply within ESP tunnel</i>   (Judgment #1)	

## Part A (ADVANCED):

- 1. HOST1 sends "ICMP Echo Request with ESP tunnel"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

# Possible Problems:



#### 5.3.2. Tunnel Mode with SGW

#### Purpose:

Verify that a NUT (End-Node) can build IPsec tunnel mode with SGW correctly (End-Node tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Tunnel Mode)

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:

HOST1 -- SGW1 ----- NUT -----> SA-I



## Security Association Database (SAD) for SA-I

•	
source address	SGW1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

# Security Policy Database (SPD) for SA-I

tunnel source address	SGW1_Link1
tunnel destination address	NUT_Link0
source address	Link2
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

## Security Association Database (SAD) for SA-0

cocarrey hossoriation bacasacs (only for on o	
source address	NUT_Link0
destination address	SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

## Security Policy Database (SPD) for SA-0

tunnel source address	NUT_Link0
tunnel destination address	SGW1_Link1
source address	NUT_Link0
destination address	Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Packets:

# ICMP Echo Request within ESP tunnel

IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST1_Link2
	Destination Address	NUT_Link0
ICMP	Туре	128 (Echo Request)

# ICMP Echo Reply within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link2
ICMP	Type	129 (Echo Reply)



#### Procedure:

SGW1_Link1(TN)	Target (NUT)	
		T1 '''
 	>  ICMP Echo Request from HOS. 	<i>II within ESP</i> tunnel
i 	ICMP Echo Reply to HOST1 w	ithin ESP tunnel
	(Judgment #1)	

## Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request from HOST1 within ESP tunnel"
- 2. Observe the packet transmitted by NUT

## Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

## Possible Problems:

None.



#### 5.3.3. Select SPD for 2 Hosts behind 1 SGW

## Purpose:

Verify that a NUT (End-Node) can build IPsec tunnel mode with SGW correctly (End-Node tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Tunnel Mode)

: N/A SGW

#### References:

- [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 SA1-I

country househarten bacasacs (ons) for one i	
SGW1_Link1	
NUT_Link0	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbcin01	
HMAC-SHA1	
ipv6readylogsha1in01	

# Security Policy Database (SPD) for SA1-I

tunnel source address	SGW1_Link1
tunnel destination address	NUT_Link0
source address	HOST1_Link2
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA1-0

Cocal Let Mode Later Database (Chb) Tot Office	
source address	NUT_Link0
destination address	SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA1-0

tunnel source address	NUT_Link0
tunnel destination address	SGW1_Link1
source address	NUT_Link0
destination address	H0ST1_Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Security Association Database (SAD) for SA2-I

document in bucusado (one) for one i	
SGW1_Link1	
NUT_Link0	
0x3000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbcin02	
HMAC-SHA1	
ipv6readylogsha1in02	

#### Security Policy Database (SPD) for SA2-I

SGW1_Link1
NUT_Link0
HOST2_Link2
NUT_Link0
any
in
ESP
tunnel

# Security Association Database (SAD) for SA2-0

COCCUTE TO THE CONTROL OF THE CALL OF	
source address	NUT_Link0
destination address	SGW1_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD) for SA2-0

tunnel source address	NUT_Link0
tunnel destination address	SGW1_Link1
source address	NUT_Link0
destination address	HOST2_Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Packets:

# ICMP Echo Request from HOST1 within ESP tunnel

IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST1_Link2
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST1 within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link2
ICMP	Type	129 (Echo Reply)



# ICMP Echo Request from HOST2 within ESP tunnel

Temm Lerre Mequees Trem Meet L Within Ler Sammer		
IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
IP Header	Source Address	HOST2_Link2
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST2 within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	SGW1_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
IP Header	Source Address	NUT_Link0
	Destination Address	HOST2_Link2
ICMP	Type	129 (Echo Reply)



#### Procedure:

SGW1_Link1(TN)	Target (NUT)
	 >  ICMP Echo Request from HOST1 within ESP tunne/
 	<i>ICMP Echo Reply to HOST1 within ESP tunnel</i>   (Judgment #1)
 	 >  ICMP Echo Request from HOST2 within ESP tunne  
   	<i>ICMP Echo Reply to HOST2 within ESP tunnel</i>   (Judgment #2)

#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request from HOST1 within ESP tunnel"
- 2. Observe the packet transmitted by NUT
- 3. SGW1 sends "ICMP Echo Request from HOST2 within ESP tunnel"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel". Step-4 (Judgment #2):

NUT transmits the packet "ICMP Echo Reply to HOST2 within ESP tunnel".

#### Possible Problems:

None.



# **5.3.4. Tunnel Mode Padding**

## Purpose:

Verify that a NUT (End-Node) supports padding & padding byte handling (End-Node Tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Tunnel Mode)

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:

HOST1 -- SGW1 ----- NUT -----> SA-I <----- SA-0



## Security Association Database (SAD) for SA-I

•	
source address	SGW1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

# Security Policy Database (SPD) for SA-I

tunnel source address	SGW1_Link1
tunnel destination address	NUT_Link0
source address	Link2
destination address	NUT_Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA-0

Occurred Nococration Database (OND) for on o	
source address	NUT_Link0
destination address	SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

# Security Policy Database (SPD) for SA-0

• • • • • • • • • • • • • • • • • • • •	
tunnel source address	NUT_Link0
tunnel destination address	SGW1_Link1
source address	NUT_Link0
destination address	Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Packets:

# ICMP Echo Request within ESP tunnel 1

IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Padding	sequential
	Padding Length	7
IP Header	Source Address	HOST1_Link2
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)
	Data Length	7

# ICMP Echo Request within ESP tunnel 2

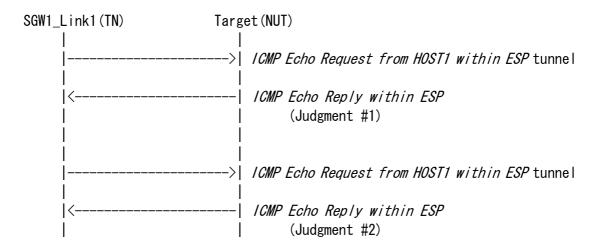
IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Padding	sequential
	Padding Length	255
IP Header	Source Address	HOST1_Link2
	Destination Address	NUT_Link0
ICMP	Туре	128 (Echo Request)
	Data Length	7



# ICMP Echo Reply within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
	Padding Length	7+8n (0 <= n <= 31)
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link2
ICMP	Туре	129 (Echo Reply)
	Data Length	7

#### Procedure:



#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request from HOST1 within ESP tunnel"
- 2. Observe the packet transmitted by NUT
- 3. SGW1 sends "ICMP Echo Request from HOST1 within ESP tunnel"
- 4. Observe the packet transmitted by NUT



## Observable Results:

## Part A:

Step-2 (Judgment #1):

NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel". Step-4 (Judgment #2):

NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel".

# Possible Problems:

None.



# **5.3.5.** Tunnel Mode TFC Padding

## Purpose:

Verify that a NUT (End-Node) supports TFC Padding (End-Node tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node: ADVANCED (This test is required for all End-Node NUTs which support

Tunnel Mode and IPsec v3)

SGW : N/A

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:

HOST1 -- SGW1 ----- NUT -----> SA-I



# Security Association Database (SAD) for SA-I

Cocal Let Modern Pacasaco (Chs) Tot Ch I		
source address	SGW1_Link1	
destination address	NUT_Link0	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

SGW1_Link1
NUT_Link0
Link2
NUT_Link0
any
in
ESP
tunnel

# Security Association Database (SAD) for SA-0

dead it is necessial in bacabase (shb) it is on e		
source address	NUT_Link0	
destination address	SGW1_Link1	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

•	
tunnel source address	NUT_Link0
tunnel destination address	SGW1_Link1
source address	NUT_Link0
destination address	Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Packets:

# ICMP Echo Request within ESP tunnel \* TFC Padded

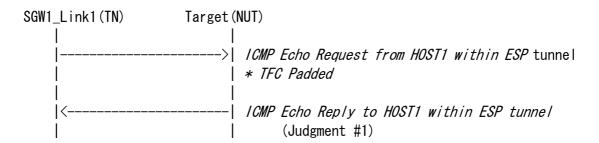
IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	H0ST1_Link2
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply within ESP tunnel

IP Header	Source Address	NUT_Link0
	Destination Address	SGW1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link2
ICMP	Type	129 (Echo Reply)



#### Procedure:



## Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request from HOST1 within ESP tunne! \* TFC Padded"
- 2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

## Possible Problems:

None.



# 6. SGW Test

This Chapter describes the test specification for SGW. The test specification consists of 2 parts. One is regarding "IPsec Architecture" and another part is regarding to "Encryption and Authentication Algorithms".

# 6.1. Architecture

# Scope:

Following tests focus on IPsec Architecture.

## Overview:

Tests in this section verify that a node properly process and transmit based on the Security Policy Database and Security Association Database.



#### **6.1.1. Select SPD**

## Purpose:

Verify that a NUT (SGW) selects appropriate SPD (SGW tunnel mode, ESP=3DES-CBC)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



## Security Association Database (SAD) for SA1-I

source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA1-I

tunnel source address	SGW1_Link2
tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA1-0

Cood it y Accordation Database (CAD) for OAT C		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA1-0

• • • • • • • • • • • • • • • • • • • •	
tunnel source address	NUT_Link1
tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Security Association Database (SAD) for SA2-I

source address	SGW2_Link2	
destination address	NUT_Link1	
SPI	0x3000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcin02	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in02	

### Security Policy Database (SPD) for SA2-I

tunnel source address	SGW2_Link2
tunnel destination address	NUT_Link1
source address	Link4
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA2-0

occurry hosperation batabase (shb) for the sh		
source address	NUT_Link1	
destination address	SGW2_Link2	
SPI	0x4000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out2	

# Security Policy Database (SPD) for SA2-0

, ,	
tunnel source address	NUT_Link1
tunnel destination address	SGW2_Link2
source address	Link0
destination address	Link4
upper spec	any
direction	out
protocol	ESP
mode	tunnel



## Packets:

# ICMP Echo Request within SA1's ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST2

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST2

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within SA1's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



# ICMP Echo Request within SA2's ESP

IP Header	Source Address	SGW2_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
IP Header	Source Address	H0ST4_Link4
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST4

IP Header	Source Address	HOST4_Link4
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST4

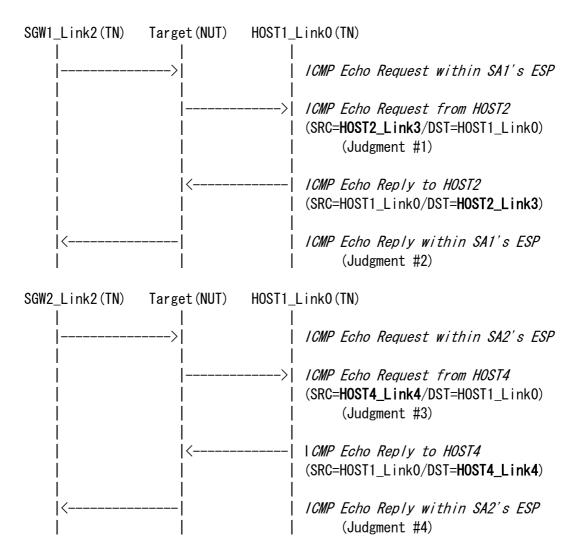
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST4_Link4
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within SA2's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW2_Link2
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST4_Link4
ICMP	Type	129 (Echo Reply)



#### Procedure:



#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within SA1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within SA2's ESP" (originally from HOST4)
- 6. Observe the packet transmitted by NUT
- 7. HOST1 sends "ICMP Echo Reply to HOST4"
- 8. Observe the packet transmitted by NUT



## Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "/CMP Echo Request from HOST2"
Step-4 (Judgment #2):
NUT transmits "/CMP Echo Reply within SA1's ESP"
Step-6 (Judgment #3):
NUT transmits "/CMP Echo Request from HOST4"
Step-8 (Judgment #4):
NUT transmits "/CMP Echo Reply within SA2's ESP"
```

## Possible Problems:

None.



# **6.1.2. Select SPD (ICMP Type)**

## Purpose:

Verify that a NUT (SGW) selects appropriate SPD (SGW tunnel mode, ESP=3DES-CBC)

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support IPsec

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



## Security Association Database (SAD) for SA1-I

occurred Macada (Ma) Tot Offi		
SGW1_Link2		
NUT_Link1		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcin01		
HMAC-SHA1		
ipv6readylogsha1in01		

#### Security Policy Database (SPD) for SA1-I

1 11	00/14 1 1 1 0
tunnel source address	SGW1_Link2
tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

## Security Association Database (SAD) for SA1-0

decar ity hooderaction bacabase (onb) for one o		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA1-0

tunnel source address	NUT_Link1	
tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	ICMPv6 Echo Request	
direction	out	
protocol	ESP	
mode	tunnel	



## Security Association Database (SAD) for SA2-I

Codi its in the contraction business (chb, its chb i		
SGW1_Link2		
NUT_Link1		
0x3000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcin02		
HMAC-SHA1		
ipv6readylogsha1in02		

#### Security Policy Database (SPD) for SA2-I

SGW1_Link2
NUT_Link1
Link3
Link0
ICMPv6 Echo Reply
in
ESP
tunnel

# Security Association Database (SAD) for SA2-0

documents house rather bacabass (Shb) for the		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x4000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout2	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out2	

# Security Policy Database (SPD) for SA2-0

• • • • • • • • • • • • • • • • • • • •	
tunnel source address	NUT_Link1
tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	ICMPv6 Echo Reply
direction	out
protocol	ESP
mode	tunnel



## Packets:

# ICMP Echo Request within SA1-I's ESP

	Tomi Zerie Medaece Within Offi T & Zer		
IP Header	Source Address	SGW1_Link2	
	Destination Address	NUT_Link1	
ESP	SPI	0x1000	
	Algorithm	3DES-CBC	
	Key	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
IP Header	Source Address	HOST2_Link3	
	Destination Address	HOST1_Link0	
ICMP	Type	128 (Echo Request)	

# ICMP Echo Request from HOST2

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST2

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within SA2-0's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



# ICMP Echo Request to HOST2

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	128 (Echo Rquest)

# ICMP Echo Request within SA1-0's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply within SA2-1's ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply from HOST2

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	129 (Echo Reply)



#### Procedure:

SGW1_Link2(TN)	Target (NUT)	HOST1_LinkO(TN)
         		ICMP Echo Request within SA1-I's ESP
        <	  <       	
SGW1 Link2(TN)	Target (NUT)	HOST1_LinkO(TN)
	<u> </u>	<i>ICMP Echo Request to HOST2</i>   (SRC=HOST1_Link0/DST= <b>HOST2_Link3</b> )
  <	!	
	   	<i>ICMP Echo Request within SA1-0's ESP</i>   (Judgment #3)
 	     >	•

#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within SA1-I's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT
- 5. HOST1 sends "ICMP Echo Request to HOST2"
- 6. Observe the packet transmitted by NUT
- 7. SGW1 sends "ICMP Echo Reply within SA2-1's ESP" (originally from HOST2)
- 8. Observe the packet transmitted by NUT



## Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Request from HOST2"
Step-4 (Judgment #2):
NUT transmits "ICMP Echo Reply within SA2-0's ESP"
Step-6 (Judgment #3):
NUT transmits "ICMP Echo Request within SA1-0's ESP"
Step-8 (Judgment #4):
NUT transmits "ICMP Echo Reply from HOST2"
```

## Possible Problems:

None.



## 6.1.3. Select SPD for 2 Hosts behind 1 SGW

## Purpose:

Verify that a NUT (SGW) selects appropriate SPD (SGW tunnel mode, ESP=3DES-CBC)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



# Security Association Database (SAD) for SA1-I

Coodiney Accordance Database (CAD) for CAT 1	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA1-I

tunnel source address	SGW1_Link2	
tunnel destination address	NUT_Link1	
source address	HOST2_Link3	
destination address	Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	
protocol	ESP	

# Security Association Database (SAD) for SA1-0

decarry necestration bacasage (ens) for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA1-0

tunnel source address	NUT_Link1
tunnel destination address	SGW1_Link2
source address	Link0
destination address	HOST2_Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# Security Association Database (SAD) for SA2-I

Court by Moderation Bucusado (CMB) 101 GMZ 1	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x3000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin02
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in02

#### Security Policy Database (SPD) for SA2-I

SGW1_Link2
NUT_Link1
HOST3_Link3
Link0
any
in
ESP
tunnel

# Security Association Database (SAD) for SA2-0

decar it is necessial to the contraction but about the contraction but	
source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD) for SA2-0

tunnel source address	NUT_Link1
tunnel destination address	SGW1_Link2
source address	Link0
destination address	HOST3_Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



### Packets:

# ICMP Echo Request within SA1's ESP

Tomi Zorio Nogacco Within orth o Zor		
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST2

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply to HOST2

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within SA1's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



## ICMP Echo Request within SA2's ESP

7		
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
IP Header	Source Address	HOST3_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Request from HOST3

IP Header	Source Address	HOST3_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply to HOST3

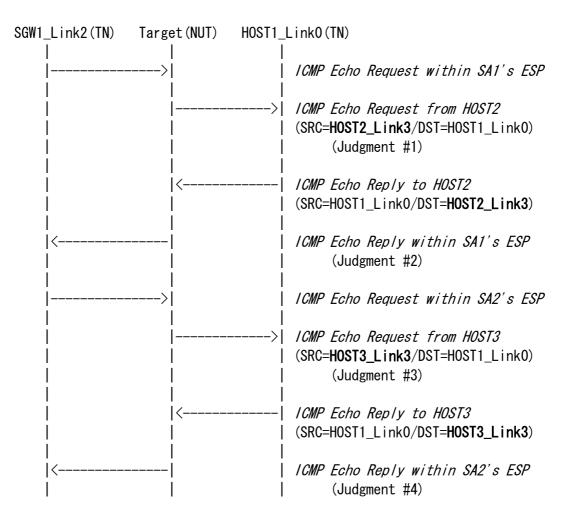
IP Header	Source Address	H0ST1_Link0
	Destination Address	HOST3_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within SA2's ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST3_Link3
ICMP	Туре	129 (Echo Reply)



#### Procedure:



#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within SA1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within SA2's ESP" (originally from HOST3)
- 6. Observe the packet transmitted by NUT
- 7. HOST1 sends "ICMP Echo Reply to HOST3"
- 8. Observe the packet transmitted by NUT



### Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "/CMP Echo Request from HOST2"
Step-4 (Judgment #2):
NUT transmits "/CMP Echo Reply within SA1's ESP"
Step-6 (Judgment #3):
NUT transmits "/CMP Echo Request from HOST3"
Step-8 (Judgment #4):
NUT transmits "/CMP Echo Reply within SA2's ESP"
```

### Possible Problems:

None.



# **6.1.4. Sequence Number Increment**

### Purpose:

Verify that a NUT (SGW) increases sequence number correctly, starting with 1. (SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



## Security Association Database (SAD) for SA-I

Total Try Modern Barasace (SMB) Tot SM T	
SGW1_Link2	
NUT_Link1	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbcin01	
HMAC-SHA1	
ipv6readylogsha1in01	

# Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

## Security Association Database (SAD) for SA-0

deduting house ration bacasace (one) for one	
source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

## Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1	
Tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



# Packets:

# ICMP Echo Request

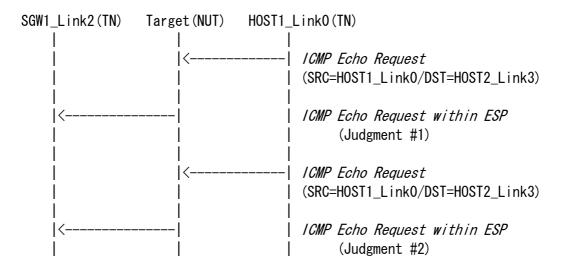
IP Header	Source Address	HOST1_LinkO
	Destination Address	HOST2_Link3
ICMP	Type	128 (Echo Request)

# ICMP Echo Request within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Sequence	$1^{st} = 1, 2^{nd} = 2$
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	128 (Echo Request)
	Data Length	7



#### Procedure:



#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Request"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

### Part A:

Step-2 (Judgment #1):

NUT transmits an "ICMP Echo Request within ESP" with an ESP Sequence number of 1  $^{\circ}$ 

Step-4 (Judgment #2):

NUT transmits an "ICMP Echo Request within ESP" with an ESP Sequence number of 2  $^{\prime\prime}$ 

### Possible Problems:

None.



# 6.1.5. Packet Too Big Transmission

### Purpose:

Verify that a NUT (SGW) transmits the ICMP Error Message (Packet Too Big) correctly. (SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

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

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



## Security Association Database (SAD) for SA-I

source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

Court by Modernation Bacasaco (CMB) for CM C		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

## Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



### Packets:

# ICMP Echo Request

Tom Lone Hogae		
IP Header	Source Address	HOST1_LinkO
	Destination Address	HOST2_Link3
	Payload Length	1460
ICMP	Type	128 (Echo Request)

# ICMP Error Message (Packet Too Big)

	<u> </u>	
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link0
ICMP	Type	2 (Packet Too Big)
	MTU	1280 <= n <= 1430 (e.g., 1280)
	Data	1232Byte of <i>ICMP Echo Request</i>

# Fragmented ICMP Echo Request to Host2 1

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	<i>1stPL</i> (=MTU-40) (e.g., 1240)
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

# Fragmented ICMP Echo Request to Host2 2

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	<i>2ndPL</i> (=1476-1stPL)
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of <i>ICMP Echo Request</i>



# Fragmented ICMP Echo Request to Host2 within ESP 1

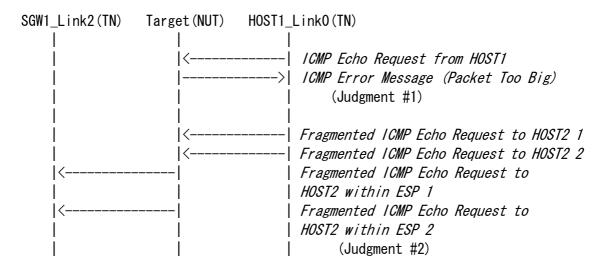
IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1stPL
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

# Fragmented ICMP Echo Request to Host2 within ESP 2

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	2ndPL
Fragment	Offset	(1stPL-8)/8
	More Flag	0
Data	Data	Rest of <i>ICMP Echo Request</i>



#### Procedure:



#### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "Fragmented ICMP Echo Request to HOST2 1" and "Fragmented ICMP Echo Request to HOST2 2"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Error Message (Packet Too Big)"

Step-4 (Judgment #2):

NUT transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

#### Possible Problems:

None.



# **6.1.6.** Packet Too Big Forwarding (Unknown Original Host)

### Purpose:

Verify that a NUT (SGW) forwards the ICMP Error Message (Packet Too Big) correctly when NUT can not determine the original host. (SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1)

### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4. Router1's interface to Link2 has an MTU value of 1356.

Set NUT's SAD and SPD as following:



### Security Association Database (SAD) for SA-I

·	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

T- 1 11	00114 1 1 1 0
Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA-0

source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

### Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



### Packets:

## ICMP Echo Request

IP Header	Source Address	HOST1_LinkO
	Destination Address	HOST2_Link3
	Payload Length	1360
ICMP	Type	128 (Echo Request)

## ICMP Error Message to NUT (Packet Too Big)

_		
IP Header	Source Address	ROUTER1_Link2
	Destination Address	NUT_Link1
ICMP	Type	2 (Packet Too Big)
	MTU	1356
	Data	1232Byte of <i>ICMP Echo Request</i>

# ICMP Error Message to HOST1 (Packet Too Big)

IP Header	Source Address	ROUTER1_Link2 or NUT_Link1
	Destination Address	HOST1_Link0
ICMP	Type	2 (Packet Too Big)
	MTU	1280 - 1286
	Data	1232Byte of <i>ICMP Echo Request</i>

## Fragmented ICMP Echo Request 1

Tragmerieea Tem Zerre Hegaeee T		
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1240
Fragment	Offset	0
	More Flag	1
ICMP	Type	128 (Echo Request)

### Fragmented ICMP Echo Request 2

rragmerraea rem zerre rragaree z		
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	136
Fragment	Offset	154
	More Flag	0
Data	Data	Rest of <i>ICMP Echo Request</i>



# ICMP Echo Request within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1360
ICMP	Type	128 (Echo Request)

# Fragmented ICMP Echo Request within ESP 1

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1240
Fragment	Offset	0
	More Flag	1
ICMP	Туре	128 (Echo Request)

## Fragmented ICMP Echo Request within ESP 2

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	136
Fragment	Offset	154
	More Flag	0
Data	Data	Rest of <i>ICMP Echo Request</i>



#### Procedure:

SGW1_Link2(TN)	ROUTER1_Link2(TN)	Target (NUT)	HOST1_LinkO(TN)	
			   <i>ICMP Echo Request</i>	<del>/</del>
  <   	        	   	ICMP Echo Request   to HOST2 within E   (Judgment #1)	ESP
		>    	   ICMP Error Message   (Packet Too Big)	e to NUT
			   <i>ICMP Echo Request</i> 	<del>/</del>
		 	>  <i>ICMP Error Messag</i>   <i>to HOST1 (Packet T</i>   (Judgment #2)	oo Big)
		  <    <	   Fragmented ICMP E   Request 1   Fragmented ICMP E   Request 2	
  <    <	        	       	Fragmented ICMP E   Request within ES   Fragmented ICMP E   Request within ES   (Judgment #3)	SP 1 Echo

### Part A (BASIC):

- 1. HOST1 sends "ICMP Echo Request"
- 2. Observe the packet transmitted by NUT
- 3. ROUTER1 sends "ICMP Error Message to NUT (Packet Too Big)"
- 4. HOST1 sends "/CMP Echo Request"
- 5. Observe the packet transmitted by NUT
- 6. HOST1 sends "Fragmented ICMP Echo Request 1" and "Fragmented ICMP Echo Request 2"
- 7. Observe the packet transmitted by NUT



### Observable Results:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Request within ESP"

Step-5 (Judgment #2):

NUT transmits "ICMP Error Message to HOST1 (Packet Too Big)"

Step-7 (Judgment #3):

NUT transmits "Fragmented ICMP Echo Request within ESP 1" and "Fragmented ICMP Echo Request within ESP 2"

### Possible Problems:

None.



# 6.1.7. Receipt of No Next Header

### Purpose:

Verify that a NUT (SGW) process the dummy packet (the protocol value 59) correctly. (SGW tunnel mode, ESP=3DES-CBC)

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support IPsec

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 ----> SA1-I <----- SA1-0



### Security Association Database (SAD) for SA1-I

Total Its Modernation Buttabaco (SMB) Tot SMT 1		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

### Security Policy Database (SPD) for SA1-I

coon reg rerreg submade (e.s., rer erri r		
tunnel source address	SGW1_Link2	
tunnel destination address	NUT_Link1	
source address	Link3	
destination address	Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

### Security Association Database (SAD) for SA1-0

decarry necestation bacasace (one) for one o		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

## Security Policy Database (SPD) for SA1-0

• • • • • • • • • • • • • • • • • • • •	
tunnel source address	NUT_Link1
tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



## Packets:

# ICMP Echo Request within SA1-I's ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST2

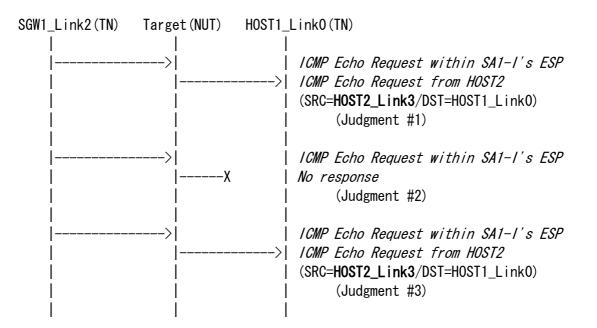
IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# No Next Header within SA1-I's ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Next Header	no next header (59)
Upper Layer	Data	empty



#### Procedure:



Part A (ADVANCED): No Next Header w/o TFC Padding

- 1. SGW1 sends "ICMP Echo Request within SA1-I's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT
- 3. SGW1 sends "No Next Header within SA1-1's ESP" (originally from HOST2). The ESP sequence number must be incremented than the packet transmitted at step 1
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2). The ESP sequence number must be incremented than the packet transmitted at step 3
- 6. Observe the packet transmitted by NUT

Part B (ADVANCED): No Next Header w/ TFC Padding

- 7. SGW1 sends "ICMP Echo Request within SA1-I's ESP" (originally from HOST2)
- Observe the packet transmitted by NUT
- 9. SGW1 sends "No Next Header within SA1-I's ESP" (originally from HOST2). The ESP sequence number must be incremented than the packet transmitted at step 7. The data in upper layer consists of random bytes as the plaintext portion.
- 10. Observe the packet transmitted by NUT
- 11. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2). The ESP sequence number must be incremented than the packet transmitted at step 9
- 12. Observe the packet transmitted by NUT



#### Observable Results:

```
Part A:
  Step-2 (Judgment #1):
    NUT transmits "ICMP Echo Request from HOST2"
 Step-4 (Judgment #2):
    NUT does not transmit any packets.
  Step-6 (Judgment #3):
    NUT transmits "ICMP Echo Request from HOST2"
Part B:
  Step-8 (Judgment #1):
    NUT transmits "ICMP Echo Request from HOST2"
  Step-10 (Judgment #2):
    NUT does not transmit any packets.
  Step-12 (Judgment #3):
    NUT transmits "ICMP Echo Request from HOST2"
```

#### Possible Problems:

None.



# 6.1.8. Bypass Policy

Dire		
rur	pose	•

Verify that a NUT (SGW) select bypass or discard policies

### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support Bypass

Policy, regardless of explicitly or implicitly)

NOTE: NUT need to pass at least either of "Bypass Policy" or "Discard Policy" tests.

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <------ SA-0



### Security Association Database (SAD) for SA-I

source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1 Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

decarry necestation bacasace (one) for on		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

## Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1	
Tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



## Packets:

# ICMP Echo Request within ESP

	Tem Lette Hedaece michili Let		
IP Header	Source Address	SGW1_Link2	
	Destination Address	NUT_Link1	
ESP	SPI	0x1000	
	Algorithm	3DES-CBC	
	Key	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
IP Header	Source Address	HOST2_Link3	
	Destination Address	HOST1_Link0	
ICMP	Type	128 (Echo Request)	

# ICMP Echo Request from HOST2

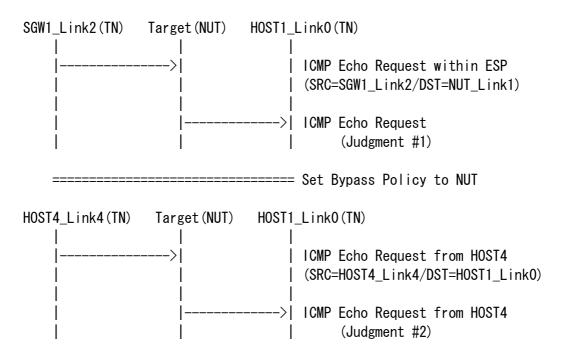
IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST4

IP Header	Source Address	HOST4_Link4
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)



#### Procedure:



Part A (ADVANCED -- except Either of Bypass or Discard Policy is required):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. Set Bypass Policy for above ICMP Echo Reply to NUT as following example
- 4. SGW1 sends "ICMP Echo Request from HOST4"
- 5. Observe the packet transmitted by NUT

Example 1: Security Policy Database (SPD) for policy=bypass (none)

source address	HOST4_Link4	
destination address	HOST1_LinkO	
upper spec	any	
direction	out	
policy	bypass (none)	

Example 2: Security Policy Database (SPD) for policy=bypass (none) as default policy

source address	any
destination address	any
upper spec	any
direction	out
policy	bypass (none)



### Observable Results:

Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Request"
Step-5 (Judgment #2):
NUT transmits "ICMP Echo Request from HOST4"

## Possible Problems:

None.



# 6.1.9. Discard Policy

Dire		
rur	pose	•

Verify that a NUT (SGW) select bypass or discard policies

### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support Discard

Policy, regardless of explicitly or implicitly)

NOTE: NUT need to pass at least either of "Bypass Policy" or "Discard Policy" tests.

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <------ SA-0



### Security Association Database (SAD) for SA-I

Total 125 Mood Table Database (CMB) 101 CM 1		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

Courtey house at the bacasacs (ons) for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

### Security Policy Database (SPD) for SA-0

coon registration (e.e., res esse		
Tunnel source address	NUT_Link1	
Tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



## Packets:

# ICMP Echo Request within ESP

,			
IP Header	Source Address	SGW1_Link2	
	Destination Address	NUT_Link1	
ESP	SPI	0x1000	
	Algorithm	3DES-CBC	
	Key	ipv6readylogo3descbcin01	
	Authentication Algorithm	HMAC-SHA1	
	Authentication Key	ipv6readylogsha1in01	
IP Header	Source Address	HOST2_Link3	
	Destination Address	HOST1_Link0	
ICMP	Type	128 (Echo Request)	

# ICMP Echo Request

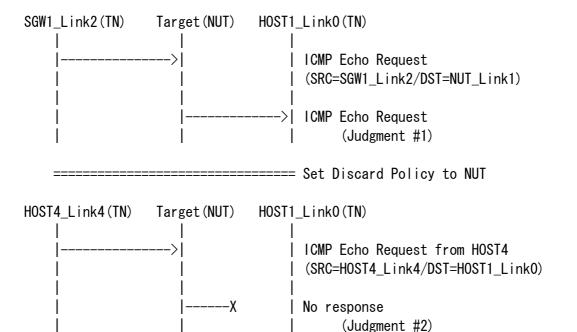
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST4

IP Header	Source Address	HOST4_Link4
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)



#### Procedure:



Part A (ADVANCED -- except Either of Bypass or Discard Policy is required):

- 1. SGW1 sends "ICMP Echo Request"
- 2. Observe the packet transmitted by NUT
- 3. Set discard policy for above ICMP Echo Reply to NUT as following example
- 4. HOST4 sends "ICMP Echo Request from HOST4"
- 5. Observe the packet transmitted by NUT

Example 1: Security Policy Database (SPD) for policy=discard

	` ' '
source address	HOST4_Link4
destination address	HOST1_Link0
upper spec	any
direction	out
policy	discard

Example 2: Security Policy Database (SPD) for policy-discard as default policy

source address	any
destination address	any
upper spec	any
direction	out
policy	discard



### Observable Results:

Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Request"
Step-5 (Judgment #2):
NUT does not transmits any packets.

## Possible Problems:

None.



# 6.1.10. Tunnel Mode Padding

### Purpose:

Verify that a NUT (SGW) supports padding & padding byte handling (SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



## Security Association Database (SAD) for SA-I

country house action bacasage (only for on t	
SGW1_Link2	
NUT_Link1	
0x1000	
tunnel	
ESP	
3DES-CBC	
ipv6readylogo3descbcin01	
HMAC-SHA1	
ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

Courtey housestation bacasace (one) for one	
source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

## Security Policy Database (SPD) for SA-0

• • • • • • • • • • • • • • • • • • • •	
Tunnel source address	NUT_Link0
Tunnel destination address	HOST1_Link1
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
	Padding	Sequential
	Padding Length	7+8n (0 <= n <= 31)
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)
	Data Length	7

# ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Туре	128 (Echo Request)

# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
	Padding	Sequential
	Padding Length	7+8n (0 <= n <= 31)
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)
	Data Length	7



SGW1_Link2(TN)	Target (NUT)	HOST1_LinkO(TN)
   	 >  	   <i>ICMP Echo Request within ESP</i>   (padding length is 7)
	   	>   <i>ICMP Echo Request</i>   (SRC=HOST2_Link3/DST=HOST1_Link0)   (Judgment #1)
	  < 	<i>ICMP Echo Reply</i>   (SRC=HOST1_Link0/DST=HOST2_Link3)
  < 	      	<i>ICMP Echo Reply within ESP</i>   (Judgment #2)
 	>    	<i>ICMP Echo Request within ESP</i>   (padding length is 255)
	   	>   <i>ICMP Echo Request</i>   (SRC=HOST2_Link3/DST=HOST1_Link0)   (Judgment #3)
	  < 	<i>ICMP Echo Reply</i>   (SRC=HOST1_Link0/DST=HOST2_Link3)
  <	 	<i>ICMP Echo Reply within ESP</i>   (Judgment #4)

#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within ESP" (Padding Length=7)
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within ESP" (Padding Length=255)
- 6. Observe the packet transmitted by NUT
- 7. HOST1 sends "ICMP Echo Reply"
- 8. Observe the packet transmitted by NUT



### Observable Results:

```
Part A:
Step-2 (Judgment #1):
NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
NUT transmits "ICMP Echo Reply within ESP"
Step-6 (Judgment #3):
NUT transmits "ICMP Echo Request"
Step-8 (Judgment #4):
NUT transmits "ICMP Echo Reply within ESP"
```

### Possible Problems:



# 6.1.11. TFC Padding

# Purpose:

Verify that a NUT (SGW) supports TFC Padding (End-Node transport mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support IPsec

v3)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA1-I <----- SA1-O



### Security Association Database (SAD) for SA1-I

decertify hooderation bacasage (only) for one i		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA1-I

tunnel source address	SGW1_Link2
tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA1-0

decarry necestation bacasace (one) for one o		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA1-0

tunnel source address	NUT_Link1	
tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



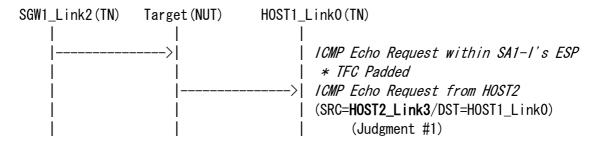
#### ICMP Echo Request within SA1-I's ESP \* TFC Padded

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

#### ICMP Echo Request from HOST2

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

#### Procedure:



### Part A (ADVANCED):

1. SGW1 sends "ICMP Echo Request within SA1-1's ESP \* TFC Padded" (originally from HOST2)

185

2. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):

NUT transmits "ICMP Echo Request from HOST2"

#### Possible Problems:





# 6.1.12. Non-Registered SPI

### Purpose:

Verify that a NUT (SGW) can behave when No valid Security Association is configured.

# Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



### Security Association Database (SAD) for SA-I

· · · · · · · · · · · · · · · · · · ·	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2	
Tunnel destination address	NUT_Link1	
source address	Link3	
destination address	Link0	
upper spec	any	
direction	in	
protocol	ESP	
mode	tunnel	

### Security Association Database (SAD) for SA-0

Codd Try Moddoracton Database (CMD) Tot ON C		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP algorithm key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1	
Tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



# ICMP Echo Request within ESP 1

Tom Zone megacoc	=	
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Sequence Number	1
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Туре	128 (Echo Request)

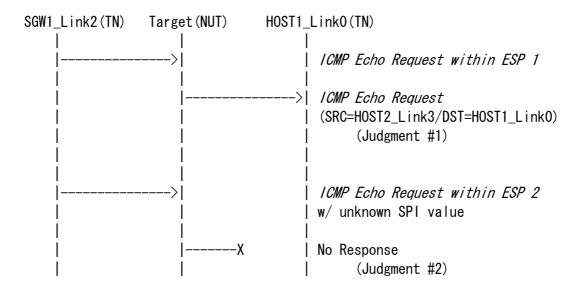
# ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request within ESP 2 with non-registered SPI

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x9000 (different from SA-I's
		SPD)
	Sequence Number	1
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)





#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within ESP 1"
- 2. Observe the packet transmitted by NUT
- 3. SGW1 sends "ICMP Echo Request within ESP 2"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT does not transmit any packets.

#### Possible Problems:



### 6.1.13. ICV

### Purpose:

Verify that a NUT (SGW) can detect the modification by examining the ICV (SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1)

#### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



### Security Association Database (SAD) for SA-I

country moderation business (only not on the		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcin01	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

T- 1 11	00114 1 1 1 0
Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

country modernation business (only for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1	
Tunnel destination address	SGW1_Link2	
source address	Link0	
destination address	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



# ICMP Echo Request within ESP 1

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Sequence number	1
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)
	Data	"PadLen is zero"

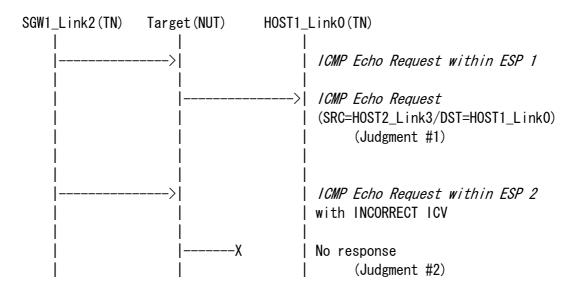
# ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	H0ST1_Link0
ICMP	Type	128 (Echo Request)
	Data	"PadLen is zero"

# ICMP Echo Request within ESP 2

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Sequence number	2
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
	ICV	aaaaaaaaa
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)
	Data	"cracked"





#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within ESP 1"
- 2. Observe the packet transmitted by NUT
- 3. SGW1 sends "ICMP Echo Request with ESP 2" (with INCORRECT ICV)
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT does not transmit any packets.

#### Possible Problems:



# 6.1.14. Tunnel Mode with End-Node

### Purpose:

Verify that a NUT (SGW) can build IPsec tunnel mode with End-Node correctly, ESP=3DES-CBC

### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 3

Set NUT's SAD and SPD as following:

HOST2 ----- NUT -- HOST1 -----> SA-I <----- SA-0



### Security Association Database (SAD) for SA-I

Total 125 Moderation Basabace (CMB) 101 CM 1	
source address	HOST2_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

HOST2_Link2
NUT_Link1
HOST2_Link2
HOST1_Link0
any
in
ESP
tunnel

# Security Association Database (SAD) for SA-0

source address	NUT_Link1
destination address	H0ST2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

### Security Policy Database (SPD) for SA-0

tunnel source address	NUT_Link1
tunnel destination address	H0ST2_Link2
source address	H0ST1_Link0
destination address	H0ST2_Link2
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP tunnel

IP Header	Source Address	HOST2_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	H0ST2_Link2
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request

IP Header	Source Address	H0ST2_Link2
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

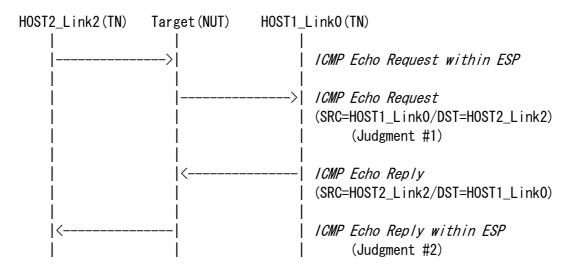
# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	H0ST2_Link2
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP tunnel

IP Header	Source Address	NUT_Link1
	Destination Address	H0ST2_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link2
ICMP	Type	129 (Echo Reply)





#### Part A (BASIC):

- 1. HOST2 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:



# **6.2.** Algorithm Test

### Scope:

Following tests focus on Encryption and Authentication Algorithms.

### Overview:

Tests in this section verify that the NUT properly decrypt the received packet s and encrypts the transmitting packets using Encryption algorithms specified in the SAD.

And they verify that the NUT properly processes the authentication algorithms specified in the SAD.



# 6.2.1. Tunnel Mode ESP=3DES-CBC HMAC-SHA1

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

SGW tunnel mode, ESP=3DES-CBC HMAC-SHA1

### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### References:

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

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <----- SA-0



### Security Association Database (SAD) for SA-I

·	•
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

# Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

occurrey hococration bacasace (one) for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

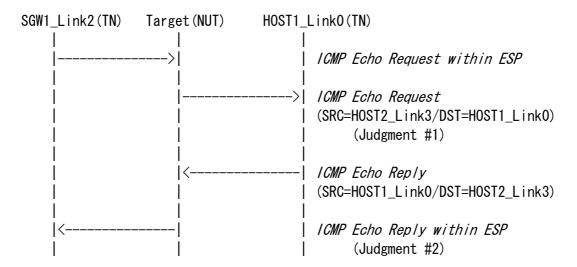
# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)





#### Part A (BASIC):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:



# 6.2.2. Tunnel Mode ESP=3DES-CBC AES-XCBC

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

SGW tunnel mode, ESP=3DES-CBC AES-XCBC

### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support AES-XCBC

as an authentication algorithm)

#### References:

- [RFC2451]
- [RFC3566]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <----- SA-0



### Security Association Database (SAD) for SA-I

order to the contact of business (only to the the		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcin01	
ESP authentication	AES-XCBC	
ESP authentication key	ipv6readaesxin01	

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1 Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

### Security Association Database (SAD) for SA-0

document in bacasage (one) for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcout1	
ESP authentication	AES-XCBC	
ESP authentication key	ipv6readaesxout1	

# Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesxin01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

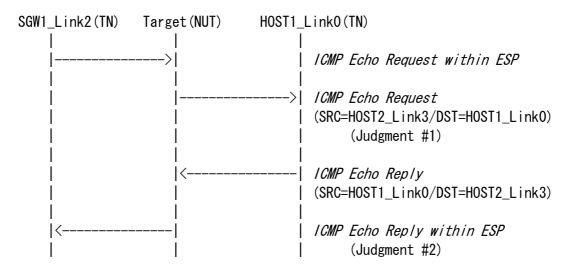
# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesxout1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)





#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:



# 6.2.3. Tunnel Mode ESP=3DES-CBC NULL

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

SGW tunnel mode, ESP=3DES-CBC NULL

### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support NULL

as an authentication algorithm)

#### References:

- [RFC2410]
- [RFC2451]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 ----> SA-I <----- SA-0



### Security Association Database (SAD) for SA-I

Court by Moode tacton Basabase (CMB) for CMT		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	3DES-CBC	
ESP key	ipv6readylogo3descbcin01	
ESP authentication	NULL	
ESP authentication key		

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1 Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA-0

source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout1
ESP authentication	NULL
ESP authentication key	

### Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	NULL
	Authentication Key	
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

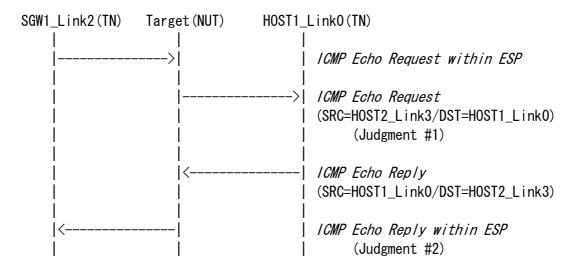
# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	NULL
	Authentication Key	
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)





#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:



# 6.2.4. Tunnel Mode ESP=AES-CBC (128-bit) HMAC-SHA1

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

SGW tunnel mode, ESP=AES-CBC (128-bit) HMAC-SHA1

### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CBC

(128-bit) as an encryption algorithm)

#### References:

- [RFC2404]
- [RFC3602]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <----- SA-0



### Security Association Database (SAD) for SA-I

•	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaescin01
ESP authentication algorithm	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

# Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

# Security Association Database (SAD) for SA-0

Cocalley Mocociation battabase (OND) for ON C		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	AES-CBC(128-bit)	
ESP key	ipv6readaescout1	
ESP authentication algorithm	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

# Security Policy Database (SPD) for SA-0

• • • • • • • • • • • • • • • • • • • •	
Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

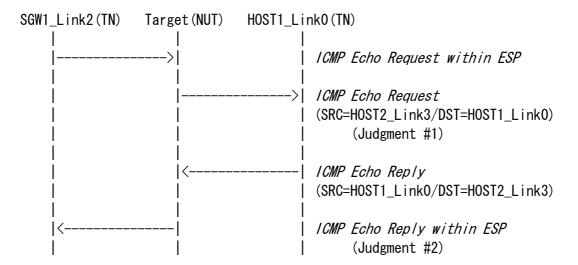
# ICMP Echo Reply

IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)





#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:



#### 6.2.5. Tunnel Mode ESP=AES-CTR HMAC-SHA1

D.,		n	_	_	_	٠
Pu	ľ	μ	u	ঠ	u	•

SGW tunnel mode, ESP=AES-CTR HMAC-SHA1

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support AES-CTR

as an encryption algorithm)

#### References:

- [RFC3686]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 ----> SA-I <----- SA-0



#### Security Association Database (SAD) for SA-I

codi iti, ilocociation bacasaco (cile	,
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogaescin01
ESP authentication algorithm	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1 Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

## Security Association Database (SAD) for SA-0

source address	NUT_Link1
destination address	SGW1_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogaescout1
ESP authentication algorithm	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out1

#### Security Policy Database (SPD) for SA-0

• • • • • • • • • • • • • • • • • • • •	
Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



#### Packets:

## ICMP Echo Request within ESP

Source Address	SGW1_Link2
Destination Address	NUT_Link1
SPI	0x1000
Algorithm	AES-CTR
Key	ipv6readylogaescin01
Authentication Algorithm	HMAC-SHA1
Authentication Key	ipv6readylogsha1in01
Source Address	HOST2_Link3
Destination Address	HOST1_Link0
Type	128 (Echo Request)
	Destination Address SPI Algorithm Key Authentication Algorithm Authentication Key Source Address Destination Address

## ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply

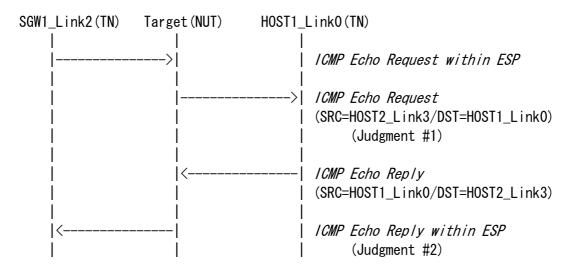
IP Header	Source Address	HOST1_LinkO
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

## ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogaescout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



#### Procedure:



#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:

None.



## 6.2.6. Tunnel Mode ESP=NULL HMAC-SHA1

Dir	2000	
rui	pose	•

SGW tunnel mode, ESP=NULL HMAC-SHA1

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support NULL

as an encryption algorithm)

#### References:

- [RFC2404]
- [RFC2410]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <------ SA-0



#### Security Association Database (SAD) for SA-I

occurry hose cratical bacasace (chb) for the	
source address	SGW1_Link2
destination address	NUT_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication algorithm	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1_Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

#### Security Association Database (SAD) for SA-0

decarry necestration bacasage (ens) for en		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	NULL	
ESP key		
ESP authentication algorithm	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

#### Security Policy Database (SPD) for SA-0

• • • • • • • • • • • • • • • • • • • •	
Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



#### Packets:

## ICMP Echo Request within ESP

Tem Zerie Hegaeee II Eliin Zer		
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Request

IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply

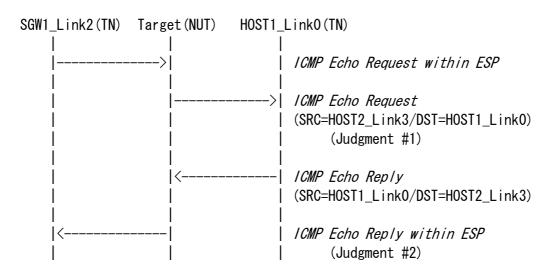
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

## ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	NULL
	Key	
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



#### Procedure:



#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1):
 NUT transmits "ICMP Echo Request"
Step-4 (Judgment #2):
 NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:

None.



## 6.2.7. Tunnel Mode ESP= CAMELLIA-CBC (128-bit) HMAC-SHA1

Dire	2000	•
гuг	pose	٠

SGW tunnel mode, ESP= CAMELLIA-CBC HMAC-SHA1

#### Category:

End-Node : N/A

SGW : ADVANCED (This test is required for all SGW NUTs which support

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

#### References:

- [RFC2404]
- [RFC4301]
- [RFC4303]
- [RFC4305]
- [RFC4312]
- [RFC4443]

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:

HOST2\_Link3 -- SGW1 ------ NUT -- HOST1\_Link0 -----> SA-I <----- SA-0



#### Security Association Database (SAD) for SA-I

· · ·		
source address	SGW1_Link2	
destination address	NUT_Link1	
SPI	0x1000	
mode	tunnel	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP key	ipvcamelliacin01	
ESP authentication algorithm	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1in01	

#### Security Policy Database (SPD) for SA-I

Tunnel source address	SGW1 Link2
Tunnel destination address	NUT_Link1
source address	Link3
destination address	Link0
upper spec	any
direction	in
protocol	ESP
mode	tunnel

#### Security Association Database (SAD) for SA-0

occurred hosestation bacasass (one) for one		
source address	NUT_Link1	
destination address	SGW1_Link2	
SPI	0x2000	
mode	tunnel	
protocol	ESP	
ESP algorithm	CAMELLIA-CBC(128-bit)	
ESP key	ipvcamelliacout1	
ESP authentication algorithm	HMAC-SHA1	
ESP authentication key	ipv6readylogsha1out1	

## Security Policy Database (SPD) for SA-0

Tunnel source address	NUT_Link1
Tunnel destination address	SGW1_Link2
source address	Link0
destination address	Link3
upper spec	any
direction	out
protocol	ESP
mode	tunnel



#### Packets:

## ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipvcamelliacin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

## ICMP Echo Reply

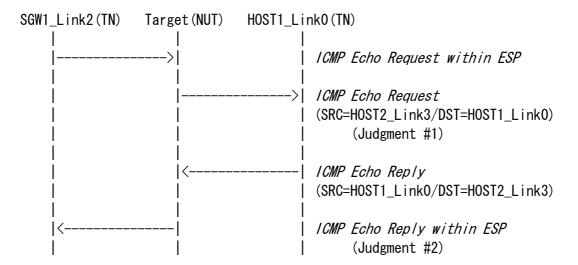
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)

## ICMP Echo Reply within ESP

IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipvcamelliacout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	129 (Echo Reply)



#### Procedure:



#### Part A (ADVANCED):

- 1. SGW1 sends "ICMP Echo Request within ESP"
- 2. Observe the packet transmitted by NUT
- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Observable Results:

#### Part A:

Step-2 (Judgment #1): NUT transmits "ICMP Echo Request" Step-4 (Judgment #2): NUT transmits "ICMP Echo Reply within ESP"

#### Possible Problems:

None.



# Appendix-A annex-5.1.2 for the passive node

This appendix describes alternative methods to perform Test 5.1.2 on the passive node which doesn't have the application to send ICMPv6 Echo Request.



# 1.1.using UDP application to invoke ICMPv6 Destination

## Unreachable (Port unreachable)

#### **Requirements:**

- 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)
HOST1 ----- transport ----- NUT
               ---- spi=0x1000 -----> SA1-I ICMPv6 Echo Request
           <----- spi=0x2000 ----- SA2-0 ICMPv6 Echo Reply
<----- spi=0x3000 ----- SA3-0 ICMPv6 Destination Unreachable</pre>
                                                    (Port unreachable)
```



#### • SA1-I

## Security Association Database (SAD)

source address	HOST1_Link1
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

## Security Policy Database (SPD)

source address	HOST1_Link1
destination address	NUT_Link0
upper spec	ICMPv6 Echo Request
direction	inbound
protocol	ESP
mode	transport

#### • SA2-O

## Security Association Database (SAD)

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD)

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	ICMPv6 Echo Reply
direction	outbound
protocol	ESP
mode	transport



#### • SA3-O

## Security Association Database (SAD)

source address	NUT_Link0
destination address	HOST1_Link1
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout3
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out3

## Security Policy Database (SPD)

source address	NUT_Link0
destination address	HOST1_Link1
upper spec	ICMPv6 Destination Unreachable
direction	outbound
protocol	ESP
mode	transport



#### **Packets:**

## ICMPv6 Echo Request with ESP1

IPv6	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMPv6	Type	128 (Echo Request)

## ICMPv6 Echo Reply with ESP2

IPv6	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMPv6	Type	129 (Echo Reply)

## UDP packet toward closed port

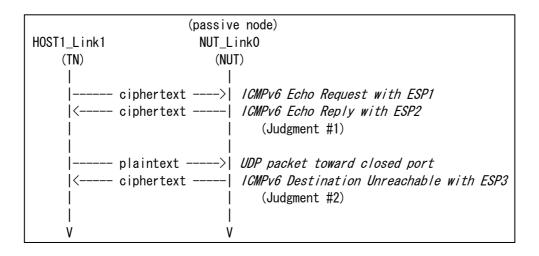
IPv6	Source Address	HOST1_Link1
	Destination Address	NUT_Link0
UDP	Source Port	Any unused port on HOST1
	Destination Port	Any closed port on NUT

#### ICMPv6 Destination Unreachable with ESP3

IPv6	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout3
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out3
ICMPv6	Type	1 (Destination Unreachable)
	Code	4 (Port unreachable)



#### **Procedure:**



#### Part A (ADVANCED):

- 1. HOST1\_Link1 sends "ICMPv6 Echo Request with ESP1" to NUT\_Link0
- 2. Observe the packet transmitted by NUT\_Link0
- 3. HOST1\_Link1 sends "UDP packet toward closed port" to NUT\_Link0
- 4. Observe the packet transmitted by NUT\_Link0

#### **Observable Results:**

#### Part A:

Step-2 (Judgment #1):

NUT\_Link0 transmits "ICMPv6 Echo Reply with ESP2"

Step-4 (Judgment #2):

NUT\_Link0 transmits "ICMPv6 Destination Unreachable with ESP3"

#### **Possible Problems:**

None.



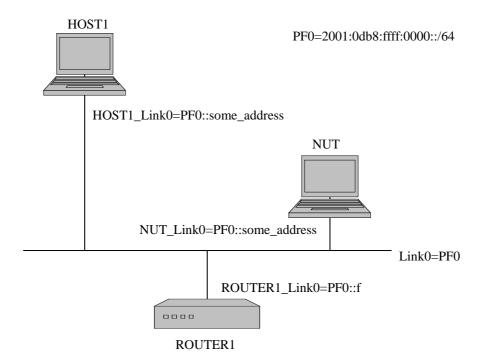
# 1.2. invoking Neighbor Unreachability Detection

#### **Requirements:**

Must respond to ICMPv6 Echo Request with ICMPv6 Echo Reply

#### **Initialization:**

Use following topology



Reboot NUT making sure it has cleared its neighbor cache. Allow time for all devices on Link0 to perform Stateless Address Autoconfiguration and Duplicate Address Detection.



- 1. Set the global address (NUT\_Link0) to NUT by RA if NUT is the host.

  Otherwise set the global address (NUT\_Link0) to NUT manually
- 2. Set MTU (1500 bytes for Link0) to NUT by RA if NUT is the host. Otherwise set MTU (1500 bytes for Link0) to NUT manually.
- 3. Set NUT's SAD and SPD as following:

(passive node)		
HOST1		
> spi=0x1000> SA1-I	ICMPv6 Echo Request	
< spi=0x2000 SA2-0	ICMPv6 Echo Reply	
< spi=0x3000 SA3-0	ICMPv6 Neighbor Solicitation	
> spi=0x4000> SA4-I	ICMPv6 Neighbor Advertisement	



#### • SA1-I

## Security Association Database (SAD)

source address	HOST1_Link0
destination address	NUT_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in01

## Security Policy Database (SPD)

source address	HOST1_Link0
destination address	NUT_Link0
upper spec	ICMPv6 Echo Request
direction	inbound
protocol	ESP
mode	transport

#### • SA2-O

## Security Association Database (SAD)

source address	NUT_Link0
destination address	HOST1_Link0
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out2

# Security Policy Database (SPD)

source address	NUT_Link0
destination address	HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	outbound
protocol	ESP
mode	transport



#### • SA3-O

## Security Association Database (SAD)

source address	NUT_Link0
destination address	HOST1_Link0
SPI	0x3000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcout3
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1out3

## Security Policy Database (SPD)

source address	NUT_Link0
destination address	HOST1_Link0
upper spec	ICMPv6 Neighbor Solicitation
direction	ipv6readylogo3descbcin01outbound
protocol	ESP
mode	transport

#### • SA4-I

## Security Association Database (SAD)

source address	HOST1_Link0
destination address	NUT_Link0
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbcin04
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1in04

## Security Policy Database (SPD)

source address	HOST1_Link0
destination address	NUT_Link0
upper spec	ICMPv6 Neighbor Advertisement
direction	inbound
protocol	ESP
mode	transport



#### **Packets:**

## ICMPv6 Neighbor Solicitation (multicast)

IPv6	Hop Limit	255
	Source Address	HOST1_Link0
	Destination Address	NUT_Link0
		(solicited-node multicast address)
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address NUT_Link0	
	Source link-layer address Option	
	Link-Layer Address: HOST1_Link0 MAC address	

## ICMPv6 Neighbor Advertisement

IPv6	Hop Limit	255
	Source Address	NUT_Link0
	Destination Address	HOST1_Link0
ICMPv6	Type	136 (Neighbor Advertisement)
	R	false (if NUT is the host)
		true (if NUT is the router)
	S	true
	0	true
	Target Address	NUT_Link0
	Target link-layer address Option	
	Link-Layer Address: NUT_Link0 MAC address	

## ICMPv6 Echo Request with ESP1

IPv6	Source Address	HOST1_Link0
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Sequence Number	1
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
ICMPv6	Type	128 (Echo Request)

## ICMPv6 Echo Reply with ESP2

IPv6	Source Address	NUT_Link0
	Destination Address	HOST1_Link0
ESP	SPI	0x2000
	Sequence Number	1
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMPv6	Type	129 (Echo Reply)



# ICMPv6 Neighbor Solicitation with ESP3

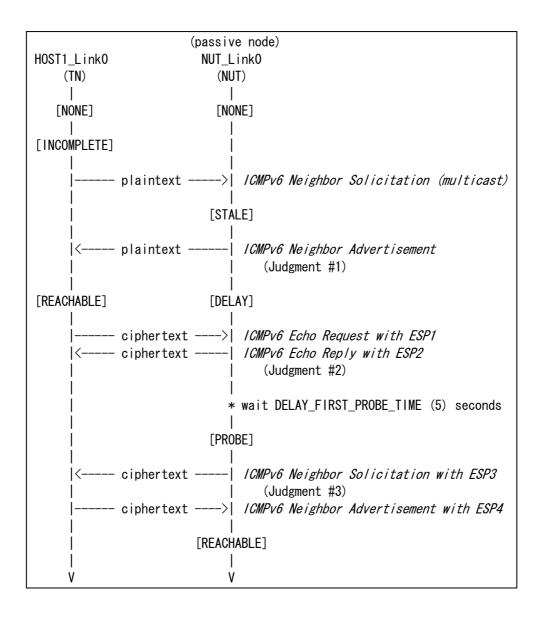
IPv6	Hop Limit	255
	Source Address	NUT_Link0
	Destination Address	HOST1_Link0
ESP	SPI	0x3000
	Sequence Number	1
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout3
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out3
ICMPv6	Type	135 (Neighbor Solicitation)
	Target Address	HOST1_Link0
	Source link-layer address Option	
	Link-Layer Address: NUT_Link0 MAC address	

# ICMPv6 Neighbor Advertisement with ESP4

IPv6	Hop Limit	255
	Source Address	HOST1_Link0
	Destination Address	NUT_Link0
ESP	SPI	0x4000
	Sequence Number	1
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcin04
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in04
ICMPv6	Type	136 (Neighbor Advertisement)
	R	false
	S	true
	0	true
	Target Address	HOST1_Link0
	Target link-layer address Option	
	Link-Layer Address: HOST1_Link0 MAC address	



#### **Procedure:**





#### Part A (ADVANCED):

- 1. HOST1\_Link0 sends "ICMPv6 Neighbor Solicitation (multicast)" to NUT Link0
- 2. Observe the packet transmitted by NUT\_Link0
- 3. HOST1\_Link0 sends "ICMPv6 Echo Request with ESP1" to NUT\_Link0
- 4. Observe the packet transmitted by NUT\_Link0
- Observe the packet transmitted by NUT\_Link0 for DELAY\_FIRST\_PROBE\_TIME (5) seconds
- 6. HOST1\_Link0 sends "ICMPv6 Neighbor Advertisement with ESP4" to NUT\_Link0

#### **Observable Results:**

# Part A: Step-2 (Judgment #1): NUT\_Link0 transmits "ICMPv6 Neighbor Advertisement" Step-4 (Judgment #2): NUT\_Link0 transmits "ICMPv6 Echo Reply with ESP2" Step-5 (Judgment #3): NUT\_Link0 transmits "ICMPv6 Neighbor Solicitation with ESP3"

#### **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.