IPv6 Rea	dy Logo	
Phase-2 Test S		
Technical I	Oocument	
Revision	າ 1.9.0	



# **MODIFICATION RECORD**

Version 1.9.0	December 09, 2008
	• Support RFC 4312 (The Camellia Cipher Algorithm and Its Use With IPsec) (Section 5.2.7, 6.2.7)
V ' 101	• Use IPv6 prefix defined in RFC 3849 for the documentation
Version 1.8.1	October 11, 2007
Version 1.8.0	<ul> <li>Remove ESN test cases (Section 5.1.12, 6.1.14)</li> <li>April 27, 2007</li> </ul>
VC131011 1. 0. 0	• Support IPsec v3
Version 1.7.7	April 6, 2006
	• Correct 5.3.4 Category
Version 1.7.6	December 22, 2005
	• Correct expected MTU value in ICMP Packet Too Big message
	for 6.1.5 Packet Too Big Forwarding.
Version 1.7.5	September 20, 2005
	• Correct the maximum MTU value for 6.1.4 Packet Too Big
	Transmission.
Version 1.7.4	June 13, 2005
V : 170	• Fix typos.
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
VE131011 1. 7. Z	• Fix typos.
Version 1.7.1	April 18, 2005
70101011 1. 7. 1	• Change Security Policy for 5.3.2.
Version 1.7	April 8, 2005
	Add Sequence Number Increment Test.
	<ul> <li>Add ICMP Error Test.</li> </ul>
Version 1.6	March 1, 2005
	• Change Keys
	<ul> <li>Add Select SPD test for tunnel mode</li> </ul>
Version 1.5	November 26, 2004
	• Change packet description of 5.1.4
Version 1.4	November 19, 2004
	Change Host to End-Node,  Pefault almostitum about the (2DEC 2DEC 1984) for the control of
	<ul> <li>Default algorithms changed to (3DES-CBC, HMAC-SHA1) for Architecture test.</li> </ul>
	<ul><li>Editorial fix</li></ul>
Version 1.3	September 24, 2004
Version 1.2	September 22, 2004
. 5. 5. 5	000000000000000000000000000000000000000



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 following IPsec related RFCs.

RFC 2404:	The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2410:	The NULL Encryption Algorithm and Its Use With IPsec
RFC 2451:	The ESP CBC-Mode Cipher Algorithms
RFC 3602:	The AES-CBC Cipher Algorithm and Its Use with IPsec
RFC 3566:	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
RFC 3686:	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)
RFC 4301:	Security Architecture for the Internet Protocol
RFC 4303:	IP Encapsulating Security Payload (ESP)
RFC 4305:	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 4312:	The Camellia Cipher Algorithm and Its Use With IPsec
RFC 4443:	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification



MODIFICATION RECORD	1
ACKNOWLEDGEMENT	3
INTRODUCTION	4
REQUIREMENTS	5
REFERENCES	8
1. Test Details	2
2. Test Topology	4
For End-Node: Transport and Tunnel Mode with End-Node Test	4
For End-Node: Tunnel Mode with SGW Test	5
For SGW: Tunnel Mode with End-Node Test	6
For SGW: Tunnel Mode Test	7
3. Description 1	9
4. Required Tests 2	0.
For End-Node: 2	1
For SGW:2	2
5. End-Node Test	.3
5.1. Architecture	23
5.1.1. Select SPD	4
5.1.2. Select SPD (ICMP Type)	9
5.1.3. Sequence Number Increment	4
5.1.4. Packet Too Big Reception	8
5.1.5. Receipt of No Next Header	-3
5.1.6. Bypass Policy4	9
5.1.7. Discard Policy5	4
5.1.8. Transport Mode Padding	9
5.1.9. Transport Mode TFC Padding	i3
5.1.10. Non-Registered SPI	7
5.1.11. ICV	1
5.2. Algorithm Test	5
5.2.1. Transport Mode ESP=3DES-CBC HMAC-SHA1	6



5.2.2	Transport Mode ESP=3DES-CBC AES-XCBC	80
5.2.3	. Transport Mode ESP=3DES-CBC NULL	84
5.2.4	. Transport Mode ESP=AES-CBC (128-bit) HMAC-SHA1	88
5.2.5	. Transport Mode ESP= AES-CTR HMAC-SHA1	92
5.2.6	. Transport Mode ESP=NULL HMAC-SHA1	96
5.2.7	. Transport Mode ESP=CAMELLIA-CBC (128-bit) HMAC-SHA	A1 100
5.3.	Tunnel Mode	104
5.3.1	Tunnel Mode with End-Node	104
5.3.2	Tunnel Mode with SGW	108
5.3.3	Select SPD for 2 Hosts behind 1 SGW	112
5.3.4	Tunnel Mode Padding	118
5.3.5	Tunnel Mode TFC Padding	123
6. SGW	Test	127
6.1.	Architecture	127
6.1.1	Select SPD	128
6.1.2	Select SPD (ICMP Type)	135
6.1.3	Select SPD for 2 Hosts behind 1 SGW	142
6.1.4	Sequence Number Increment	149
6.1.5	Packet Too Big Transmission	153
6.1.6	Packet Too Big Forwarding (Unknown Original Host)	158
6.1.7	Receipt of No Next Header	164
6.1.8	Bypass Policy	170
6.1.9	Discard Policy	175
6.1.1	0. Tunnel Mode Padding	180
6.1.1	1. TFC Padding	185
6.1.1	2. Non-Registered SPI	189
6.1.1	3. ICV	193
6.1.1	4. Tunnel Mode with End-Node	197
6.2.	Algorithm Test	201
6.2.1	. Tunnel Mode ESP=3DES-CBC HMAC-SHA1	202
6.2.2	Tunnel Mode ESP=3DES-CBC AES-XCBC	206



6.2.3.	Tunnel Mode ESP=3DES-CBC NULL	. 210
6.2.4.	Tunnel Mode ESP=AES-CBC (128-bit) HMAC-SHA1	. 214
6.2.5.	Tunnel Mode ESP=AES-CTR HMAC-SHA1	. 218
6.2.6.	Tunnel Mode ESP=NULL HMAC-SHA1	. 222
6.2.7.	Tunnel Mode ESP= CAMELLIA-CBC (128-bit) HMAC-SHA1	226



# 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

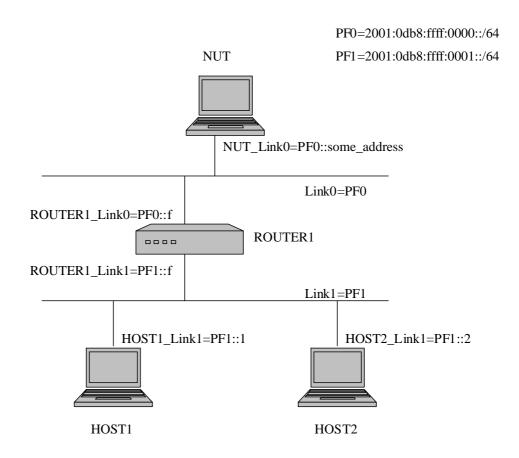


Fig. 1 Topology for End-Node: Transport and Tunnel mode with End-Node



### 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.

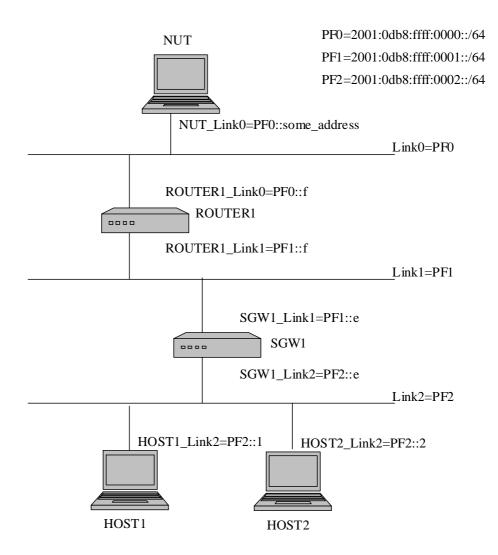


Fig. 2 Topology for End-Node: Tunnel mode with SGW



#### 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.

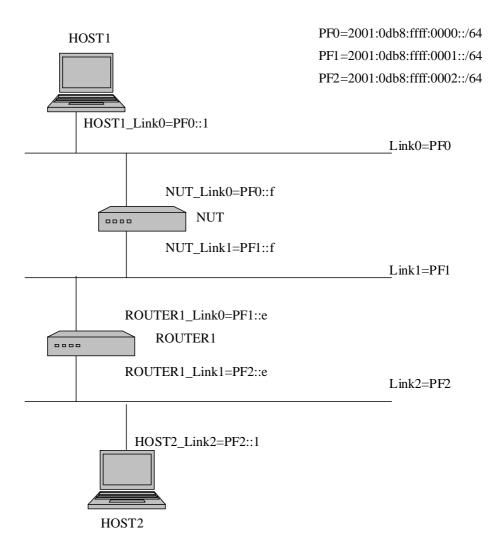


Fig. 3 Topology for SGW: Tunnel mode with End-Node



### **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



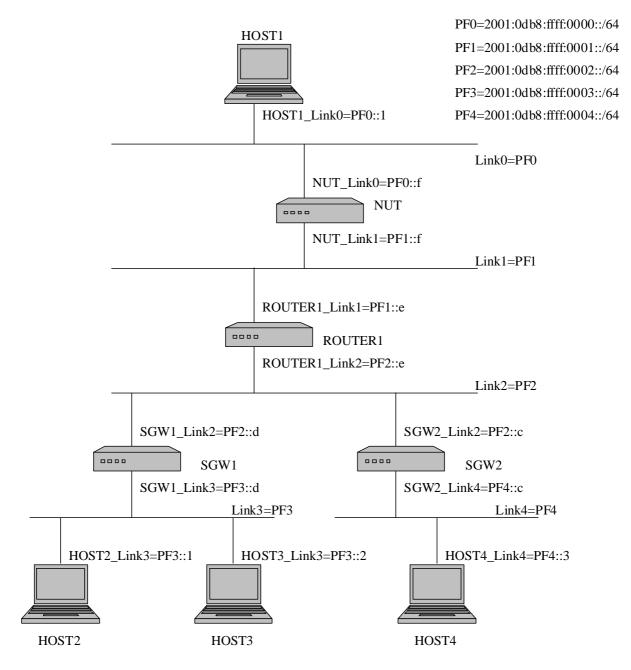


Fig. 4 Topology for SGW: Tunnel mode with SGW



# 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.

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

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

default value is used.

**Packets:** The Packets describes the simple figure of packets which is used in

the test. In this document, the packet name is represented in Italic

style font.

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

test.

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

result as the description of Judgment, the NUT passes the test.

**References:** The References section contains some parts of specification related to

19

the tests. It also shows the document names and section numbers.



# 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		
Colort CDD (ICMD Turns)	ADVANCED	IPsec v3	
Select SPD (ICMP Type)		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

### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

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



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

Total Ity Modernation Bacasace (OND) Tot ONT T		
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

Cocal Tey Medical Bacasaco (GNB) Tot GNE T		
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

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'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
ICMP	Type	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	HOST2_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMP	Type	129 (Echo Reply)



#### Procedure:

Part A: SA1

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

Part B: SA2

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with SA1's ESP".

Part B: Judgment #2

Step-4: NUT transmits "ICMP Echo Reply with SA2's ESP".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



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

Cooding Necocharion Barabaco (OND) for ONL 1		
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	Type	128 (Echo Request)

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

Telli Lerie Repriy Well one of Ler		
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

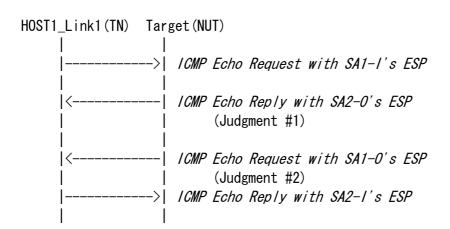
Tomi Zone negacee		
IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply with SA2-1'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	Туре	129 (Echo Reply)



#### Procedure:



Part A: SA1 (inbound)

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

Part B: SA1 (outbound)

- 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"

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with SA2-0's ESP".

Part B: Judgment #2

Step-4: NUT transmits "ICMP Echo Request with SA1-0's ESP".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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

### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



### 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



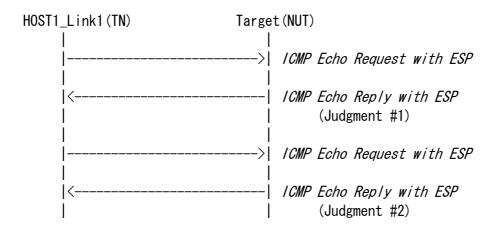
# ICMP Echo Request with ESP

Tomi Zono mogacos	Tom Love Hogadoc Witch Lov		
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	Туре	129 (Echo Reply)





- 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

#### Judgment:

Judgment #1

Step-2: NUT transmits an "ICMP Echo Reply with ESP"

with an ESP Sequence Number of 1.

Judgment #2

Step-4: NUT transmits an "ICMP Echo Reply with ESP"

with an ESP Sequence Number of 2.

### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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

#### 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:



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

order to the transfer of the t		
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



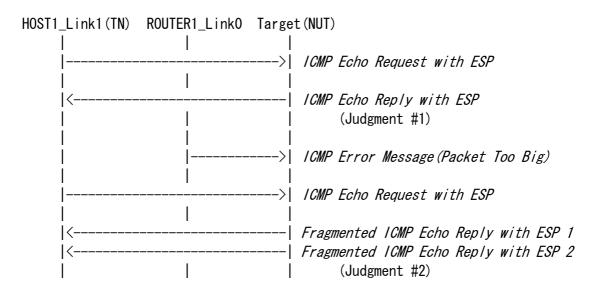
# Fragmented ICMP Echo Reply with ESP 1

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>





- 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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

Judgment #2

Step-5: NUT transmits "Fragmented ICMP Echo Reply with ESP 1"

and "Fragmented ICMP Echo Reply with ESP 2"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



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

Court by Modernation Badasacc (chb) 101 cm 1		
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

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 Hopiy II	7 217 2717 0 0 207	
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	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02



# 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	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply with SA1-0's ESP

IP Header	Source Address	NUT_Link0
	Destination Address	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out2
ICMP	Туре	129 (Echo Reply)



- (a) No Next Header w/o TFC Padding
  - Part A: SA1
    - 1. HOST1 sends "ICMP Echo Request with SA1-I's ESP"
  - 2. Observe the packet transmitted by NUT

Part B: SA1

- 3. HOST1 sends "No Next Header with SA1-0's ESP"
- 4. HOST1 sends "ICMP Echo Request with SA1-0's ESP"
- 5. Observe the packet transmitted by NUT
- (b) No Next Header w/ TFC Padding

Part A: SA1

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

Part B: SA1

- 3. HOST1 sends "No Next Header with SA1-0's ESP"
- 4. HOST1 sends "ICMP Echo Request with SA1-0's ESP"
- 5. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with SA1-0's ESP".

Part B: Judgment #2

Step-5: NUT transmits "ICMP Echo Reply with SA1-0's ESP".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 5.1.6. Bypass Policy

Dire		
rur	pose	•

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.

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



### 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

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)

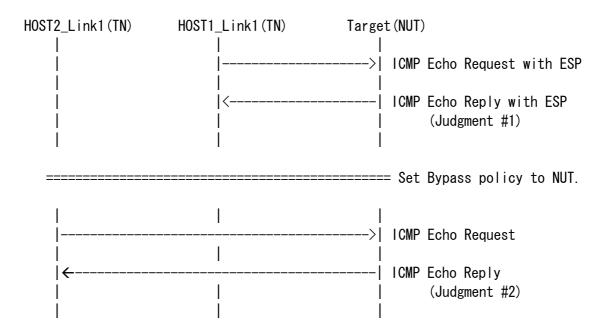
### ICMP Echo Request

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: Confirmation

- 1. Host1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

Part B: Bypass policy

3. Set Bypass policy for above ICMP Echo Request to NUT as following example

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

source address	HOST2_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)

- 4. HOST1 sends "ICMP Echo Request"
- 5. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1.

Step-2: NUT transmits "ICMP Echo Reply with ESP"

Part B: Judgment #2.

Step-5: NUT transmits "ICMP Echo Reply"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



### **5.1.7. Discard Policy**

Purpose:	Pi	J٢	po	se	
----------	----	----	----	----	--

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.

#### 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

country more actual and construction of the co	
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

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

### 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)

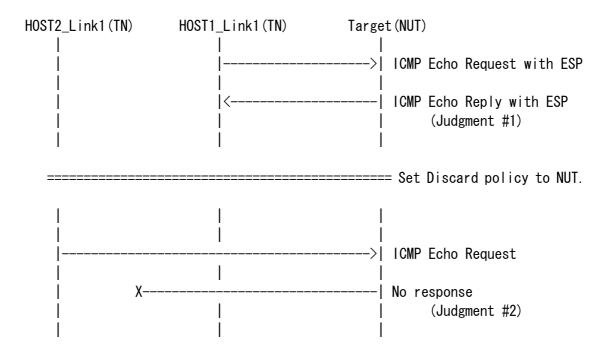
### ICMP Echo Request

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: Confirmation

- 1. Host1 sends "ICMP Echo Request with ESP"
- 2. Observe the packet transmitted by NUT

Part B: Discard policy

3. Set Discard policy for above ICMP Echo Request to NUT as following example

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	

- 4. HOST1 sends "ICMP Echo Request"
- 5. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1.

Step-2: NUT transmits "ICMP Echo Reply with ESP"

Part B: Judgment #2.

Step-5: NUT does not transmit any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 5.1.8. Transport Mode Padding

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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



### 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

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

Tem Lette Heddeed Hier Let 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
	Padding	Sequential
	Padding Length	7
ICMP	Туре	128 (Echo Request)
	Data Length	7

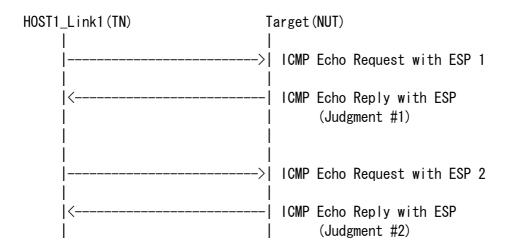
# ICMP Echo Request with ESP 2

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: Padding 7

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

Part B: Padding 255

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

Part B: Judgment #2

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

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **5.1.9. Transport Mode TFC Padding**

Durnosa		
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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



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

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	H0ST1_Link1
ESP SPI		0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
UDP	Source Port	7 (echo)
	Destination Port	10000



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

#### Judgment:

Judgment #1

Step-2: NUT transmits "UDP Echo Reply with SA1-0's ESP".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)



# 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

### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:



### 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

country more and a company to the contract of		
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	Type	128 (Echo Request)

### ICMP Echo Reply with ESP 1

Telli Zerre riepry in en Zer r		
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)

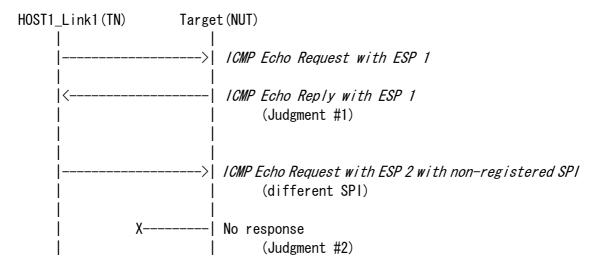
### ICMP Echo Request with ESP 2 with non-registered SPI

Tom Lone Heddeet With Let 2 With Hell 1081 oct of a city		
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: valid SA exists

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

Part B: no valid SA exists

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP 1"

Part B: Judgment #2

Step-4: NUT does not transmit any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



### 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

### 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	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

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	Type	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	Type	129 (Echo Reply)
	Data	"EchoData"

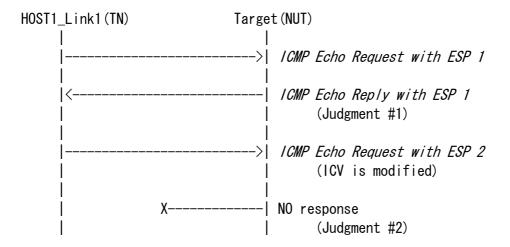
#### ICMP Echo Request with ESP 2

Tomi Lerio Reducet With Ler 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	Туре	129 (Echo Reply)





Part A: send correct packet

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

Part B: send modified packet

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP 1"

Part B: Judgment #2

Step-4: NUT does not transmit any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



# 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:			
End-Node transport mode, ESP=3DES-CBC HMAC-SHA1			
Category:			
End-Node : BASIC (A requirement for all End-Node NUTs) SGW : N/A			
Initialization:			
Use common topology described as Fig. 1			
Set NUT's SAD and SPD as following:			
HOST1_Link1 NUT> SA-I			
< SA-0			



HOST1_Link1
NUT_Link0
0x1000
transport
ESP
3DES-CBC
ipv6readylogo3descbcin01
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-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

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



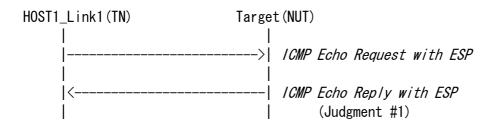
# ICMP Echo Request with ESP

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	Type	128 (Echo Request)

## 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
ICMP	Type	129 (Echo Reply)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Dir	naca	•
rui	pose	•

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

## 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-0

Total Tay Moode Table Database (only Tot on 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



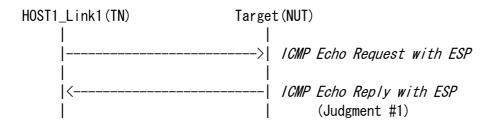
# ICMP Echo Request with ESP

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

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)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Purpo	ose:
-------	------

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

## Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

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



Total Tey house taction bacabase (OND) Tot ON T		
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		
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

country reconstruction become and construction of		
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



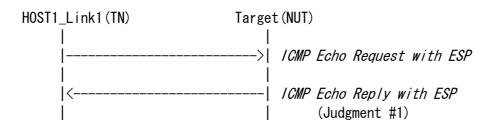
## ICMP Echo Request with ESP

Tom Love Nedacot With Lov		
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	HOST1_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbcout1
	Authentication Algorithm	NULL
	Authentication Key	
ICMP	Type	129 (Echo Reply)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

<b>Purpose</b>	•
i ui pose	•

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

#### 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	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-O

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



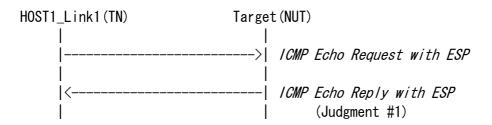
# ICMP Echo Request with ESP

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	Type	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)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

HOST1\_Link1 ----- NUT

-----> SA-I <------ SA-0

rui pose.
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
Initialization:
Use common topology described as Fig. 1
Set NUT's SAD and SPD as following:



Cocal Let Modern Pacasaco (CNS) Tot CN T		
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



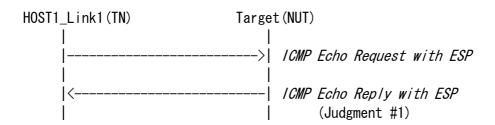
## ICMP Echo Request with ESP

Tom Lone Hogaest	11 1 2 1 2 2 1	
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	Type	128 (Echo Request)

## ICMP Echo Reply with ESP

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	Type	129 (Echo Reply)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode

With IPsec Encapsulating Security Payload (ESP)

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



# 5.2.6. Transport Mode ESP=NULL HMAC-SHA1

Purpose:
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
Initialization:
Use common topology described as Fig.1
Set NUT's SAD and SPD as following:
HOST1_Link1 NUT > SA-I



·	
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-0

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



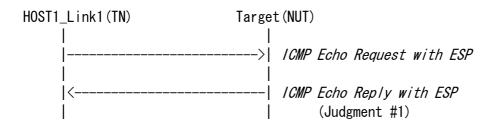
## ICMP Echo Request with ESP

remi Zerre Hegaeee Hren Zer		
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

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





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Purpo	se
-------	----

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

#### 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	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



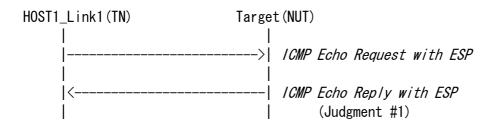
## ICMP Echo Request with ESP

Tem Lerre Requeet With Ler		
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	Туре	128 (Echo Request)

## ICMP Echo Reply with ESP

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)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Reply with ESP"

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4312: The Camellia Cipher Algorithm and Its Use With IPsec

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 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

#### Initialization:

Use common topology described as Fig. 1

Set NUT's SAD and SPD as following:

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



Total 10, 1100001401011 Batabaco (Crib) 101 011 1		
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

Total Its Modernation Bacasaco (CMB) For CM C		
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	

cooming to the parameter (c. 2) to the		
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	



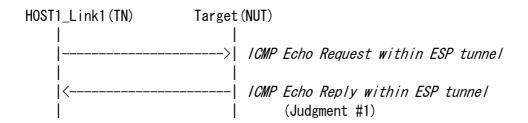
## ICMP Echo Request within ESP tunnel

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	Туре	129 (Echo Reply)





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

#### Judgment:

Judgment #1

Step-2: NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



#### **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

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



#### 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)
1	
1	
<	ICMP Echo Reply to HOST1 within ESP tunnel
	(Judgment #1)

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

#### Judgment:

Judgment #1

Step-2: NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



#### 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)

SGW : N/A

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



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

SGW1_Link1
NUT_Link0
HOST1_Link2
NUT_Link0
any
in
ESP
tunnel

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

dodn'tty hoddoration batabadd (onb) for one 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 SA1-0

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



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

Cocal Tey Moderation Bacasace (OND) Tel ONE T	
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

Coodi ity noodolation batabase (onb) it	1 6/12 6
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	Туре	129 (Echo Reply)



## ICMP Echo Request from HOST2 within ESP tunnel

		· ·
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_Li	nk1(TN)	Target (N	(NUT)
 		 	ICMP Echo Request from HOST1 within ESP tunnel
  <- 		   	CMP Echo Reply to HOST1 within ESP tunnel (Judgment #1)
   		 >  	ICMP Echo Request from HOST2 within ESP tunnel
  <- 		   	<i>ICMP Echo Reply to HOST2 within ESP tunnel</i> (Judgment #2)

Part A: SA1

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

Part B: SA2

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel".

Part B: Judgment #2

Step-4: NUT transmits the packet "ICMP Echo Reply to HOST2 within ESP tunnel".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 5.3.4. Tunnel Mode Padding

Purpose:	Pu	rp	os	е	:
----------	----	----	----	---	---

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)

: N/A SGW

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



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

Codd 12) Noocolation Batabaco (chi	3, 10, 0, 1
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

Coodi ity noccoration battabaco (onb) ita	
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

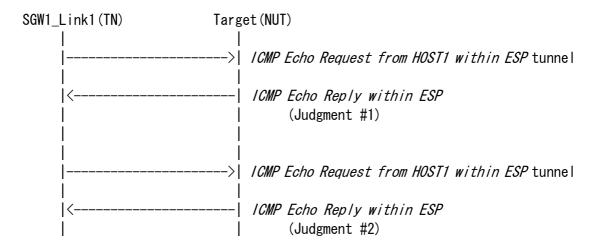


# ICMP Echo Reply within ESP tunnel

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	Type	129 (Echo Reply)
	Data Length	7



#### Procedure:



Part A: Padding 7

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

Part B: Padding 255

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel".

Part B: Judgment #2

Step-4: NUT transmits the packet "ICMP Echo Reply to HOST1 within ESP tunnel".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 5.3.5. Tunnel Mode TFC Padding

<b>Purpose</b>	:	
. a. poco	-	

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)

: N/A SGW

#### Initialization:

Use common topology described as Fig. 2

Set NUT's SAD and SPD as following:



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

Total 1 by Model Autom Bullande (CMB) 101 CM 1		
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_LinkO
source address	Link2
destination address	NUT_LinkO
upper spec	any
direction	in
protocol	ESP
mode	tunnel

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

document in the contraction bacabase (only not 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 \* TFC Padded

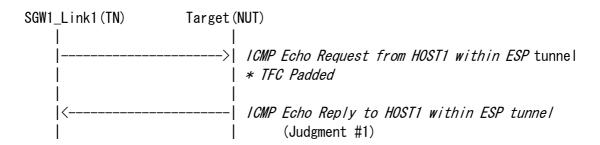
IP Header	Source Address	SGW1_Link1
	Destination Address	NUT_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST1_Link2
	Destination Address	NUT_Link0
ICMP	Type	128 (Echo Request)

# 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	Туре	129 (Echo Reply)



#### Procedure:



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

#### Judgment:

Judgment #1

Step-2: NUT transmits the packet "ICMP Echo Reply within ESP tunnel".

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 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)

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



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

Cood it y noocotation batasaco (onb) for oni 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

Court by house the buckback (only) 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	Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



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

occurred horses acres bacasace (one) for one 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

document to the decapace (one) for one of		
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	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

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

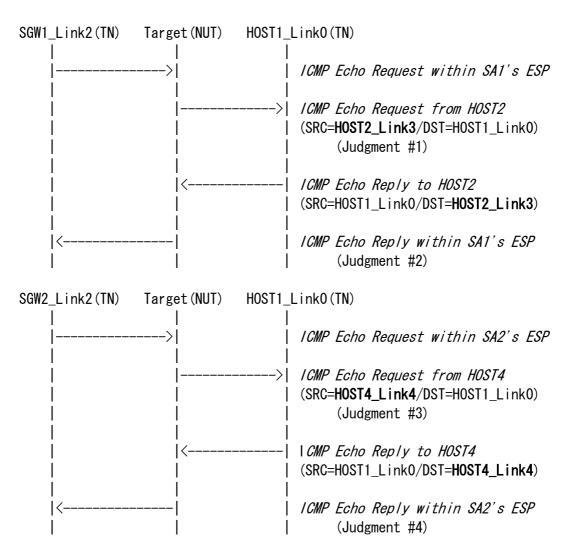
IP Header	Source Address	H0ST1_Link0
	Destination Address	HOST4_Link4
ICMP	Type	129 (Echo Reply)

# 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	Туре	129 (Echo Reply)



#### Procedure:



Part A: SA1-I

- 1. SGW1 sends "ICMP Echo Request within SA1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

Part B: SA1-0

- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT

Part C: SA2-I

- 5. SGW1 sends "ICMP Echo Request within SA2's ESP" (originally from HOST4)
- 6. Observe the packet transmitted by NUT

Part D: SA2-0

- 7. HOST1 sends "ICMP Echo Reply to HOST4"
- 8. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request from HOST2"

Part B: Judgment #2

Step-4: NUT transmits "ICMP Echo Reply within SA1's ESP"

Part C: Judgment #3

Step-6: NUT transmits "ICMP Echo Request from HOST4"

Part D: Judgment #4

Step-8: NUT transmits "ICMP Echo Reply within SA2's ESP"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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

v3)

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



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

Total 123 Modern Batabase (OND) 101 ON 1		
SGW1_Link2		
NUT_Link1		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcin01		
HMAC-SHA1		
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	ICMPv6 Echo Request	
direction	in	
protocol	ESP	
mode	tunnel	

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

Coodiney Roccondensin Database (CRD) not only		
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

occurred Naccorder Bucasaco (ons), for one 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

Court by Modern Bucusus (CMB) for CME C		
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

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 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

H	P Header	Source Address	HOST1_Link0
		Destination Address	HOST2_Link3
10	CMP	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

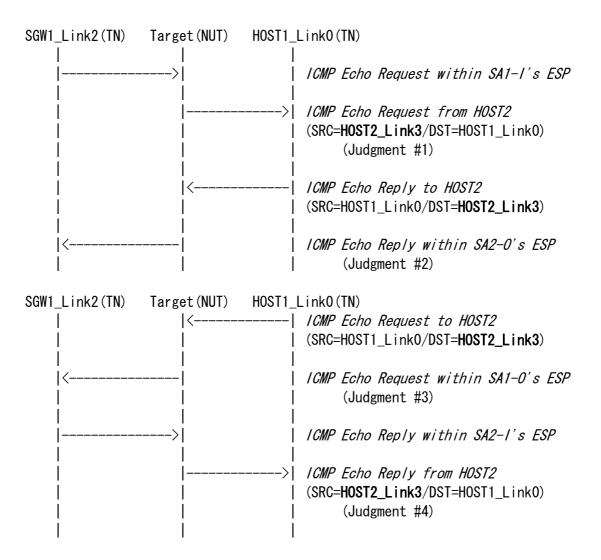
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x3000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin02
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in02
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	129 (Echo Reply)

# ICMP Echo Reply from HOST2

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



#### Procedure:



Part A: SA1-I

- 1. SGW1 sends "ICMP Echo Request within SA1-I's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

Part B: SA2-0

- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT

Part C: SA1-0

- 5. HOST1 sends "ICMP Echo Request to HOST2"
- 6. Observe the packet transmitted by NUT

Part D: SA2-I

- 7. SGW1 sends "ICMP Echo Reply within SA2-1's ESP" (originally from HOST2)
- 8. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request from HOST2"

Part B: Judgment #2

Step-4: NUT transmits "ICMP Echo Reply within SA2-0's ESP"

Part C: Judgment #3

Step-6: NUT transmits "ICMP Echo Request within SA1-0's ESP"

Part D: Judgment #4

Step-8: NUT transmits "ICMP Echo Reply from HOST2"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



#### 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)

#### 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

HOST3\_Link3 -- SGW1 ----- NUT -- HOST1\_Link0 ----- SA2-I



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

Codd 12 / Nocociation Battabaco (CNB) 101 CN1 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

country rational (craft for critical		
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	

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

Coodiney Roccondensin Bacabaco (CRB) non Orn 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	HOST2_Link3	
upper spec	any	
direction	out	
protocol	ESP	
mode	tunnel	



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

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

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

### Security Association Database (SAD) for SA2-0

decent by hose the form but abase (onb) for one of		
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

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

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

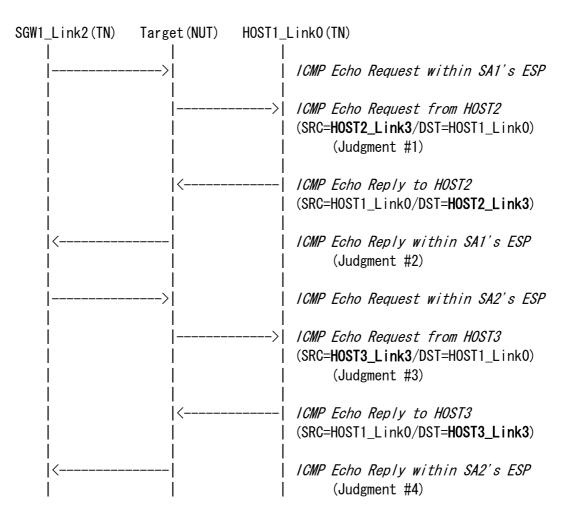
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST3_Link3
ICMP	Туре	129 (Echo Reply)

# ICMP Echo Reply within SA2's ESP

I D II I		AULT 1 1 1 4
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	Type	129 (Echo Reply)



#### Procedure:



Part A: SA1-I

- 1. SGW1 sends "ICMP Echo Request within SA1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

Part B: SA1-0

- 3. HOST1 sends "ICMP Echo Reply to HOST2"
- 4. Observe the packet transmitted by NUT

Part C: SA2-I

- 5. SGW1 sends "ICMP Echo Request within SA2's ESP" (originally from HOST3)
- 6. Observe the packet transmitted by NUT

Part D: SA2-0

- 7. HOST1 sends "ICMP Echo Reply to HOST3"
- 8. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request from HOST2"

Part B: Judgment #2

Step-4: NUT transmits "ICMP Echo Reply within SA1's ESP"

Part C: Judgment #3

Step-6: NUT transmits "ICMP Echo Request from HOST3"

Part D: Judgment #4

Step-8: NUT transmits "ICMP Echo Reply within SA2's ESP"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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)

#### 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

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

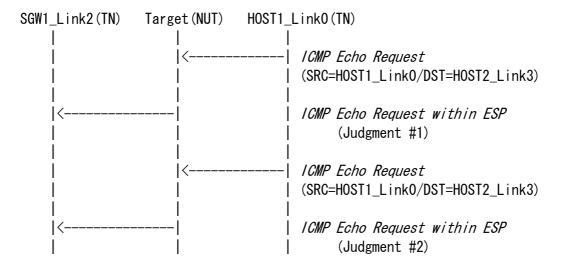
IP Header	Source Address	H0ST1_Link0
	Destination Address	HOST2_Link3
ICMP	Type	128 (Echo Request)

## 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: SA-I

1. HOST1 sends "ICMP Echo Request"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Request"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits an "ICMP Echo Request within ESP"

with an ESP Sequence number of 1

Part B: Judgment #2

Step-4: NUT transmits an "ICMP Echo Request within ESP"

with an ESP Sequence number of 2

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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)

#### 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

Occurred Necocration Database (OND) for the	
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

	Tomi Zono nogaco		
IP Header Source Address		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_LinkO
	Destination Address	H0ST2_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

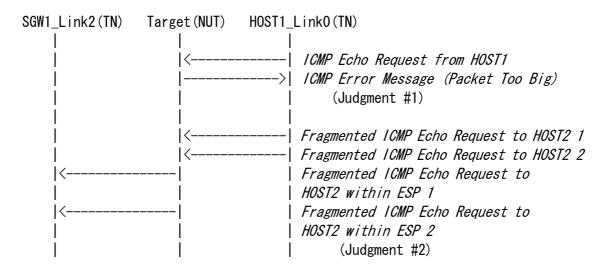
IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1stPL
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:



- 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

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Error Message (Packet Too Big)"

Judgment #2

Step-4: NUT transmits "Fragmented ICMP Echo Request within ESP 1"

and "Fragmented ICMP Echo Request within ESP 2"

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# **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)

#### 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

Country Moderation Bacasace (CMB) for the		
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

documents house the bacabass (Shb) for the		
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_Link0
	Destination Address	HOST2_Link3
	Payload Length	1360
ICMP	Туре	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

Tragmeried Tem Zerre Hegaess 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

1. agmenteed term Zente nequeee 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

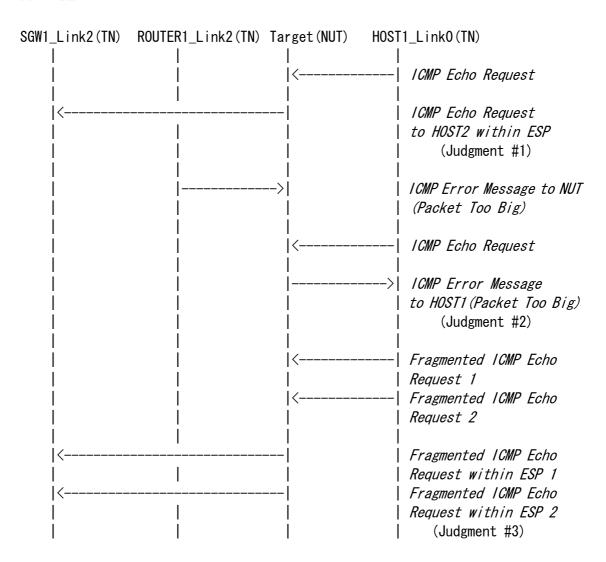
IP Header	Source Address	NUT_Link1
	Destination Address	SGW1_Link2
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcout1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1out1
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
	Payload Length	1240
Fragment	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:



- 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 "ICMP 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



#### Judgment:

Judgment #1

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

Judgment #2

Step-5: NUT transmits "ICMP Error Message to HOST1 (Packet Too Big)"

Judgment #3

Step-7: NUT transmits "Fragmented ICMP Echo Request within ESP 1"

and "Fragmented ICMP Echo Request within ESP 2"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 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

v3)

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



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

occurred hosestation bacasass (one) for one i		
SGW1_Link2		
NUT_Link1		
0x1000		
tunnel		
ESP		
3DES-CBC		
ipv6readylogo3descbcin01		
HMAC-SHA1		
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

Occurry hosporation bacasage (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 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
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0



# ICMP Echo Request within SA1-I's ESP

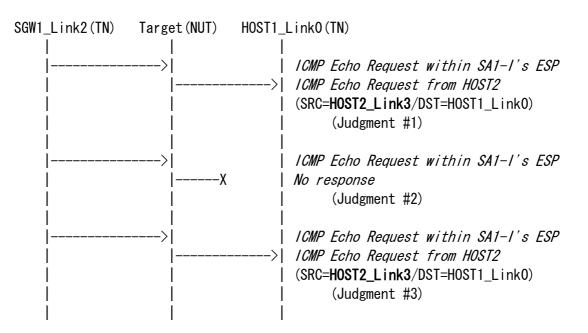
IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcin01
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1in01
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST2

IP Header	Source Address	H0ST2_Link3
	Destination Address	H0ST1_Link0
ICMP	Type	128 (Echo Request)



#### Procedure:



(a) No Next Header w/o TFC Padding

Part A: SA1-I

- 1. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

Part B: SA1-I

- 3. SGW1 sends "No Next Header within SA1-I's ESP" (originally from HOST2)
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2)
- 6. Observe the packet transmitted by NUT
- (b) No Next Header w/ TFC Padding

Part A: SA1-I

- 1. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

Part B: SA1-I

- 3. SGW1 sends "No Next Header within SA1-I's ESP" (originally from HOST2)
- 4. Observe the packet transmitted by NUT
- 5. SGW1 sends "ICMP Echo Request within SA1-1's ESP" (originally from HOST2)
- 6. Observe the packet transmitted by NUT



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request from HOST2"

Part B: Judgment #2

Step-4: NUT does not transmit any packets.

Step-6: NUT transmits "ICMP Echo Request from HOST2"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 6.1.8. Bypass Policy

<b>Purpose</b>	:	
. a. poco	-	

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.

#### 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 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

Occurry hosporation bacasage (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

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

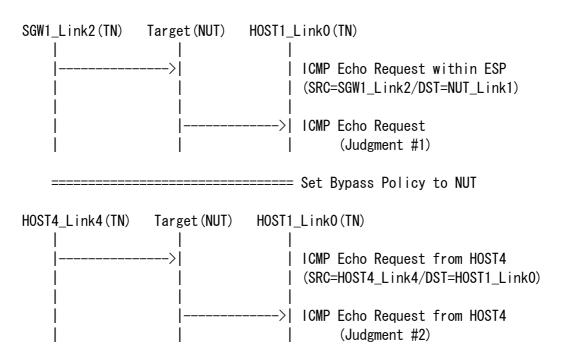
IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST4

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



#### Procedure:



Part A: Confirmation

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

Part B: Bypass Policy

- 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_Link0
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)



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

Step-5: NUT transmits "ICMP Echo Request from HOST4"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



# 6.1.9. Discard Policy

D	
Purpose	•

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.

## 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 12 /100001421011 Pasabado (one)	
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

coodinely househarton bacasace (only not on o	
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

,		
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

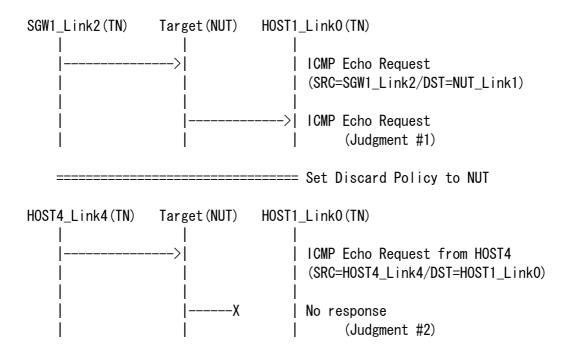
IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Request from HOST4

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



#### Procedure:



Part A: Confirmation

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

Part B: discard policy

- 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



#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

Step-5: NUT does not transmits any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification



## **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)

### 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 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

dodding hooderacion bacasade (ons) 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	

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

Tom Lone Hogaest	1	T
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	Type	128 (Echo Request)

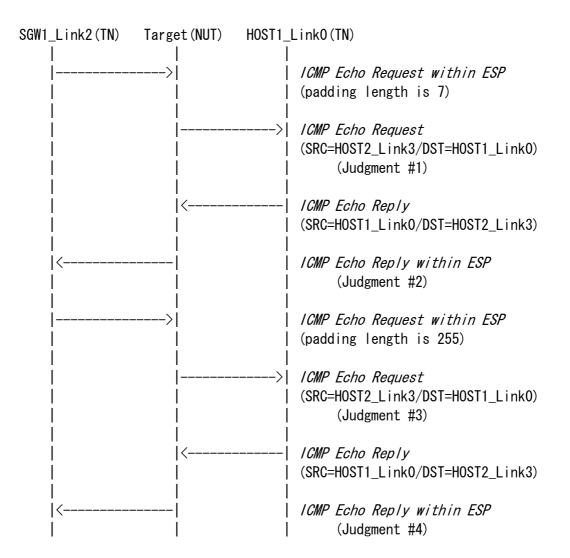
## ICMP Echo Reply

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
	Padding	Sequential
	Padding Length	7+8n (0 <= n <= 31)
IP Header	Source Address	HOST1_Link0
	Destination Address	HOST2_Link3
ICMP	Туре	129 (Echo Reply)
	Data Length	7





Part A: Padding Length is 7

- 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

Part B: Padding Length is 255

- 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



#### Judgment:

Part A: Padding Length is 7

Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Judgment #2

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

Part B: Padding Length is 255

Judgment #3

Step-6: NUT transmits "ICMP Echo Request"

Judgment #4

Step-8: NUT transmits "ICMP Echo Reply within ESP"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 6.1.11. TFC Padding

Durnosa		
Purpose	•	

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

### Category:

End-Node : N/A

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

v3)

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



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

dodding hooderacion bacabase (onb) 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

documents house the buckbase (only for one of		
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	

• • • • • • • • • • • • • • • • • • • •	
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



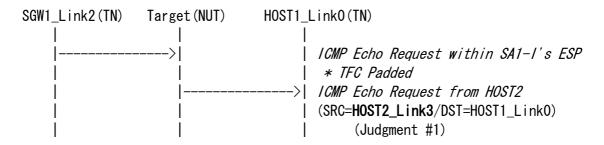
## ICMP Echo Request within SA1-I's ESP \* TFC Padded

,		
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	H0ST2_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)





- 1. SGW1 sends "ICMP Echo Request within SA1-I's ESP \* TFC Padded" (originally from HOST2)
- 2. Observe the packet transmitted by NUT

#### Judgment:

Judgment #1

Step-2: NUT transmits "ICMP Echo Request from HOST2"

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 6.1.12. Non-Registered SPI

### Purpose:

Verify that a  $\operatorname{NUT}$  (SGW) can behave when No valid Security Association is configured.

### Category:

End-Node : N/A

SGW : BASIC (A requirement for all SGW NUTs)

#### Initialization:

Use common topology described as Fig. 4

Set NUT's SAD and SPD as following:



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

occurred hoccorderon bacasaco (ons) for on 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

Total Tey Moder de Fort Database (OND) 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	

• • • • • • • • • • • • • • • • • • • •	
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)

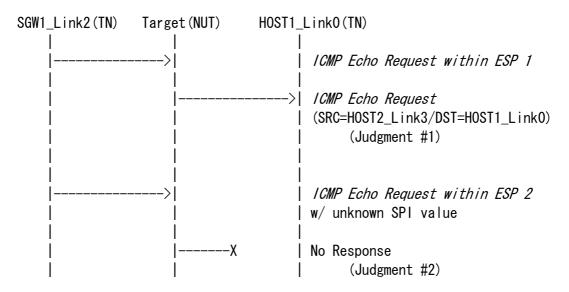
## ICMP Echo Request

IP Header	Source Address	H0ST2_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: valid SA exists

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

Part B: no valid SA exists

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

Step-4: NUT does not transmit any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 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)

## 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 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

Cocal Let Mode Later Database (CMD) Tot ON C		
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	

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"

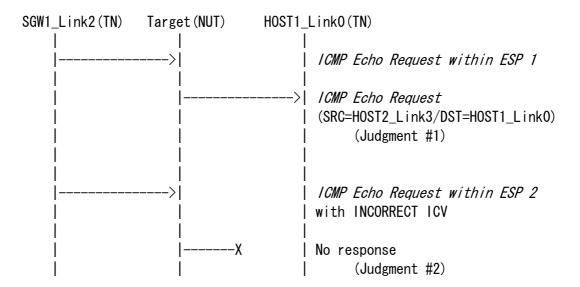
## ICMP Echo Request

IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_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: correct packet

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

Part B: modified packet

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

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

Step-4: NUT does not transmit any packets.

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 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)

### Initialization:

Use common topology described as Fig. 3

Set NUT's SAD and SPD as following:



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

Cocal Let Modoc action bacasaco (CMB) Tot CM T		
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

dead it is necessial in bacasace (one) it is on o		
source address	NUT_Link1	
destination address	HOST2_Link2	
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_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)

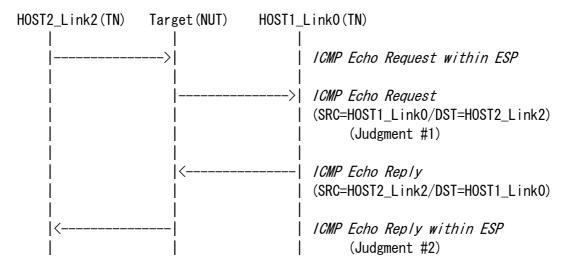
## ICMP Echo Reply

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	HOST2_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: SA-I

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

Part B: SA-0

- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



# **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



### 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

Court by Mooder at term bacasage (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	

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

Tomi Zono Negacoc II in in in zon		
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)

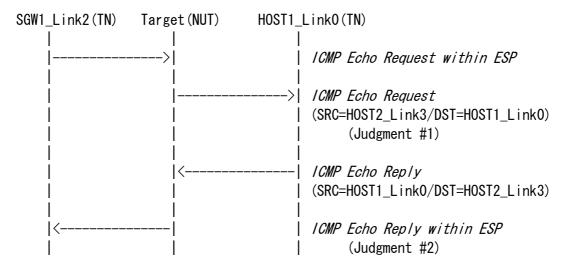
## ICMP Echo Reply

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: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Durnosa		
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)

#### 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 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

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

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

Source Address	SGW1_Link2
Destination Address	NUT_Link1
SPI	0x1000
Algorithm	3DES-CBC
Key	ipv6readylogo3descbcin01
Authentication Algorithm	AES-XCBC
Authentication Key	ipv6readaesxin01
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)

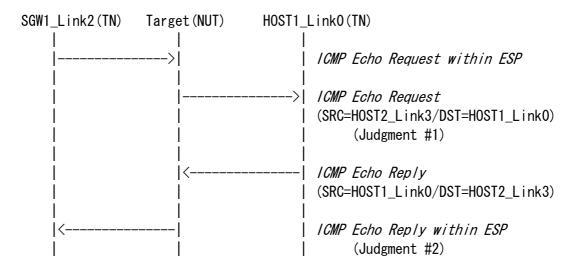
## ICMP Echo Reply

IP Header	Source Address	HOST1_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: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Purp	ose
------	-----

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)

#### 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 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	

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	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

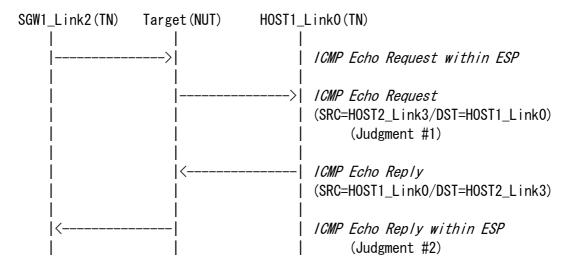
## ICMP Echo Reply

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





Part A: SA-I

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

Part B: SA-0

- 3. HOST1 sends "ICMP Echo Reply"
- 4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec

RFC 2451: The ESP CBC-Mode Cipher Algorithms

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 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)

#### 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	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

country mesocratic bacamaco (che) ici chi 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

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

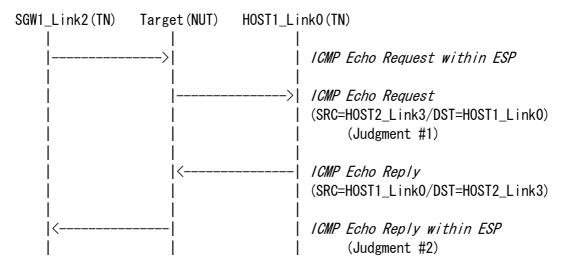
IP Header	Source Address	H0ST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply

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

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: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



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

Durnosa		
Purpose	•	

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)

### 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	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

country moderation basabase (shb) for the		
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



# ICMP Echo Request within ESP

IP Header	Source Address	SGW1_Link2
	Destination Address	NUT_Link1
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogaescin01
	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

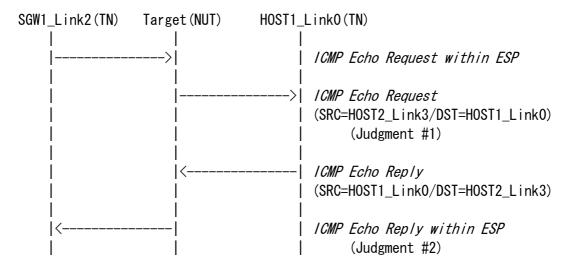
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply

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

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)





Part A: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 3686: Using Advanced Encryption Standard (AES) Counter Mode

With IPsec Encapsulating Security Payload (ESP)

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 6.2.6. Tunnel Mode ESP=NULL HMAC-SHA1

Purp	ose
------	-----

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)

### 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	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

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



# ICMP Echo Request within ESP

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

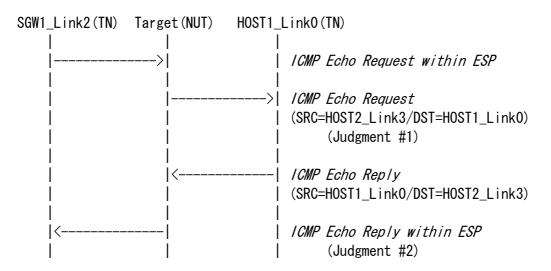
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply

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

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)





Part A: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4443: Internet Control Message Protocol (ICMPv6)



## 6.2.7. Tunnel Mode ESP= CAMELLIA-CBC (128-bit) HMAC-SHA1

### Purpose:

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)

### 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	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

Total 125 Modernation Bushades (ens.) 101 en en		
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



# 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

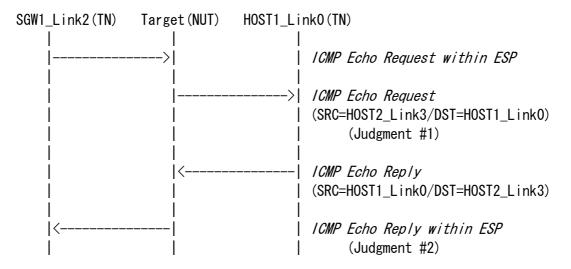
IP Header	Source Address	HOST2_Link3
	Destination Address	HOST1_Link0
ICMP	Type	128 (Echo Request)

# ICMP Echo Reply

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

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)





Part A: SA-I

1. SGW1 sends "ICMP Echo Request within ESP"

2. Observe the packet transmitted by NUT

Part B: SA-0

3. HOST1 sends "ICMP Echo Reply"

4. Observe the packet transmitted by NUT

#### Judgment:

Part A: Judgment #1

Step-2: NUT transmits "ICMP Echo Request"

Part B: Judgment #2

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

#### References:

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4305: Cryptographic Algorithm Implementation Requirements

for Encapsulating Security Payload (ESP) and Authentication Header (AH)

RFC 4312: The Camellia Cipher Algorithm and Its Use With IPsec

RFC 4443: Internet Control Message Protocol (ICMPv6)



\*

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.