IPv6 Ready Logo

Phase-2 Interoperability Test Scenario
IPsec

Technical Document

Revision 1.9.0

IPv6 Forum ***http://www.ipv6forum.org/***

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

Modification Record

Version 1.9.0	December 09, 2008
	- Support RFC 4312 (The Camellia Cipher Algorithm and Its Use With IPsec) (Section 5.1.7, 5.2.7, 5.3.7, 5.4.7)
	- Use IPv6 prefix defined in RFC 3849 for the documentation
Version 1.5.2	October 11, 2007
	- Remove ESN test cases (Section 5.1.8, 5.2.8, 5.3.8, 5.4.8)
Version 1.5.1	June 19, 2007
	- Correct subsection in Section 5.3
Version 1.5.0	April 27, 2007
	- Support IPsec v3
Version 1.4.3	October 6, 2005
	- Update Appendix
Version 1.4.2	September 30, 2005
	- Change ping direction for tunnel tests between END-Nodes
Version 1.4.1	September 22, 2005
	- Editorial fix
Version 1.4	March 1, 2005
	- Change Keys
Version 1.3	December 21, 2004
	- Correct Require table
Version 1.2	November 29, 2004
	- Add concept of End-Node rather than Host
	- Add criteria
	- Editorial fix
Version 1.1	September 30, 2004
Version 1.0	September 24, 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:

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

Introduction

The IPv6 forum plays a major role to bring together industrial actors, to develop and deploy the next generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community. Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products. To avoid confusion in the mind of customers, a globally unique logo program should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo program will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase 1:

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

Phase 2:

The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 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 following two equipment types. Every NUT can be ether of them.

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

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

Security Protocol:

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

Mode:

The mode requirement depends on the type of NUT.

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

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

Encryption Algorithm:

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

The algorithm requirement is independent from NUT type.

BASE ALGORITHM:
- 3DES-CBC

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

Authentication Algorithm:

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

The algorithm requirement is independent from NUT type.

BASE ALGORITHM:
- HMAC-SHA1

ADVANCED ALGORITHM:
- AES-XCBC-MAC-96
- NULL

Category:

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

Interoperable device requirement:

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

End-Node:

Transport Mode(BASIC): 2 devices which supports Transport Mode.
Tunnel Mode(ADVANCED): 2 devices which supports Tunnel Mode regardless of equipment type.

SGW:

Tunnel Mode(BASIC) : 2 devices which supports Tunnel Mode regardless of equipment type

References

This test specification focus on the 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

---TOC---

1. Test Details

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

Terminology:

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

Required Application:

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

IPsec Configuration:

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

Topology:

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

2. Test Topology

These logical Network Topologies are used for test samples.

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

1. Set global address to TGT_HOST1_Link0 and TGT_HOST2_Link1 by RA.
2. Make IPsec transport mode between TGT_HOST1 and TGT_HOST2.

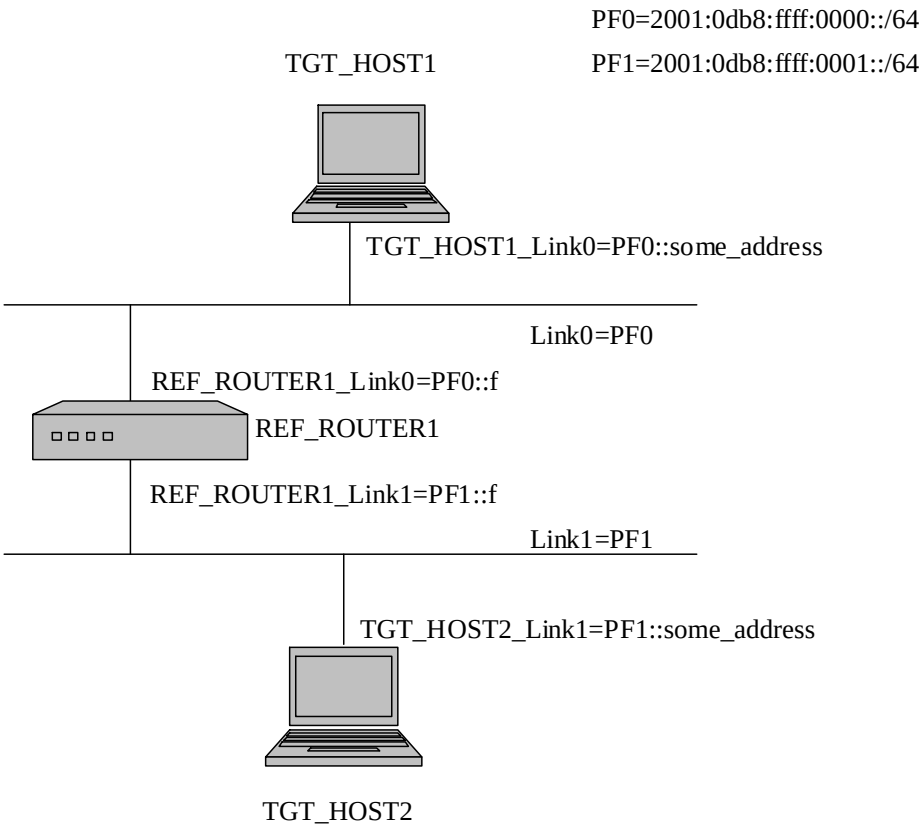


Figure 1 Topology for End-Node: Transport and Tunnel mode with End-Node

For SGW vs. SGW Tunnel Mode Test

1. Set global address to REF_HOST1_Link0 and REF_HOST2_Link3 by RA.
2. Set global address to TGT_SGW1_Link0, TGT_SGW1_Link1, TGT_SGW2_Link2, TGT_SGW2_Link3, REF_ROUTER1_Link1, REF_ROUTER1_Link2 manually.
3. Set routing table to TGT_SGW1 (REF_ROUTER1_Link1 for Link2 and Link3)
4. Set routing table to TGT_SGW2 (REF_ROUTER1_Link2 for Link0 and Link1)
5. Set routing table to REF_ROUTER1 (TGT_SGW1_Link1 for Link0, TGT_SGW2_Link2 for Link3)
6. Make IPsec tunnel mode between TGT_SGW1 and TGT_SGW2.

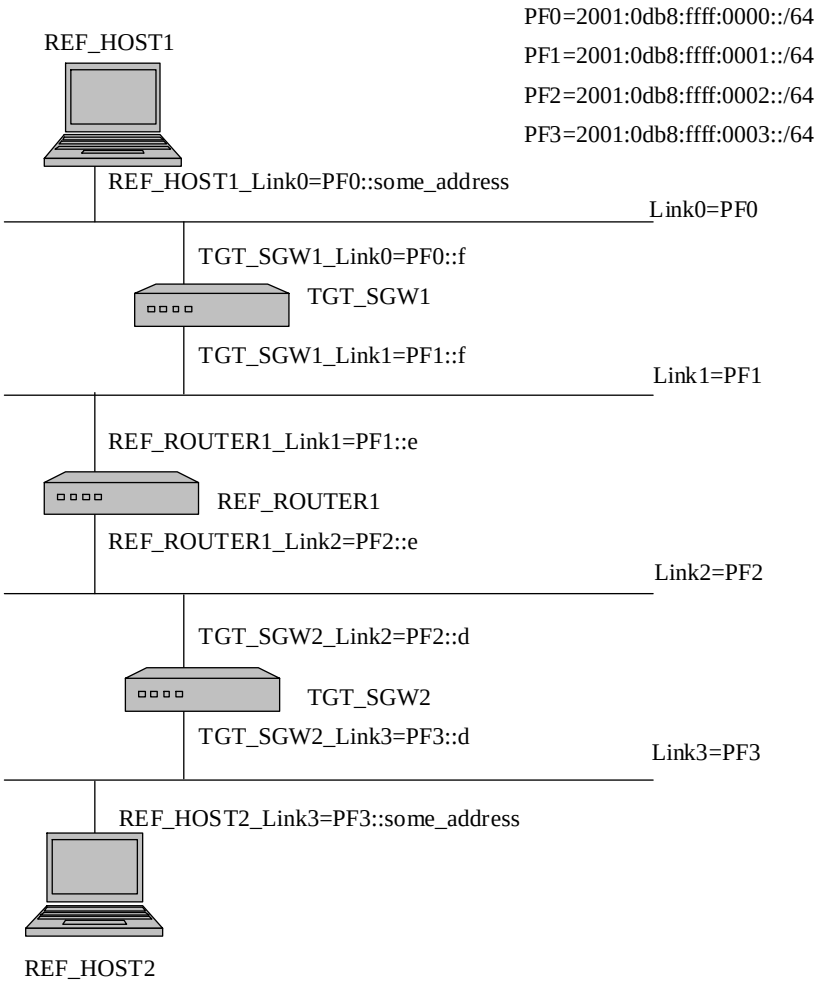


Figure 2 Topology for SGW: Tunnel mode with SGW

For End-Node vs. SGW Tunnel Mode Test

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

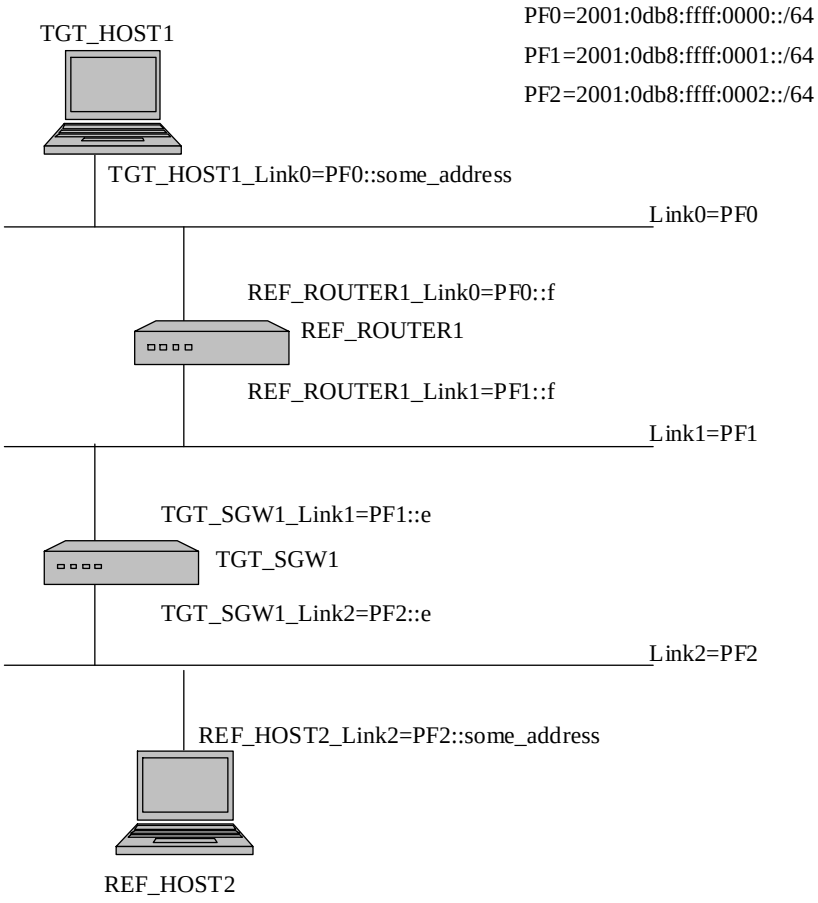


Figure 3 Topology for End-Node: Tunnel mode with SGW

3. Description

Each test scenario consists of following parts.

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

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

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: Reference RFC list containing description related to the test.

4. Required Tests

The following table describes which tests are required.

Focused Interface	Test Title	Device Type	
		End-Node	SGW
End-Node vs. End-Node (Transport)	Transport Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	N/A
	Transport Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	N/A
	Transport Mode: ESP=3DES-CBC NULL	ADVANCED	N/A
	Transport Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	Transport Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	N/A
	Transport Mode: ESP=NULL HMAC-SHA1	ADVANCED	N/A
	Transport Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	Transport Mode: Select SPD (ICMP Type)	ADVANCED *3	N/A
	Transport Mode: dummy packet handling	ADVANCED	N/A
	Transport Mode: TFC padding	ADVANCED *4	N/A
SGW vs. SGW (Tunnel) *1	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	N/A	BASIC
	Tunnel Mode: ESP=3DES-CBC AES-XCBC	N/A	ADVANCED
	Tunnel Mode: ESP=3DES-CBC NULL	N/A	ADVANCED
	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	N/A	ADVANCED
	Tunnel Mode: ESP=AES-CTR HMAC-SHA1	N/A	ADVANCED
	Tunnel Mode: ESP=NULL HMAC-SHA1	N/A	ADVANCED
	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	N/A	ADVANCED
	Tunnel Mode: ESP=Select SPD (ICMP Type)	N/A	ADVANCED *3
	Tunnel Mode: ESP=dummy packet	N/A	ADVANCED
	Tunnel Mode: ESP=TFC padding	N/A	ADVANCED

Focused Interface	Test Title	Device Type	
		End-Node	SGW
End-Node vs. SGW (Tunnel) *1, *2	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	BASIC
	Tunnel Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	ADVANCED
	Tunnel Mode: ESP=3DES-CBC NULL	ADVANCED	ADVANCED
	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	ADVANCED
	Tunnel Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	ADVANCED
	Tunnel Mode: ESP=NULL HMAC-SHA1	ADVANCED	ADVANCED
	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	ADVANCED
	Tunnel Mode: ESP=Select SPD (ICMP Type)	ADVANCED *3	ADVANCED *3
	Tunnel Mode: ESP=dummy packet handling	ADVANCED	ADVANCED
	Tunnel Mode: ESP=TFC padding	ADVANCED	ADVANCED
End-Node vs. End-Node (Tunnel) *1, *2	Tunnel Mode: ESP=3DES-CBC HMAC-SHA1	BASIC	N/A
	Tunnel Mode: ESP=3DES-CBC AES-XCBC	ADVANCED	N/A
	Tunnel Mode: ESP=3DES-CBC NULL	ADVANCED	N/A
	Tunnel Mode: ESP=AES-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	Tunnel Mode: ESP=AES-CTR HMAC-SHA1	ADVANCED	N/A
	Tunnel Mode: ESP=NULL HMAC-SHA1	ADVANCED	N/A
	Tunnel Mode: ESP=CAMELLIA-CBC(128-bit) HMAC-SHA1	ADVANCED	N/A
	Tunnel Mode: ESP=Select SPD (ICMP Type)	ADVANCED *3	N/A
	Tunnel Mode: ESP=dummy packet handling	ADVANCED	N/A
	Tunnel Mode: ESP=TFC padding	ADVANCED	N/A

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

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

*3: This test should be done by using ICMP.

*4: This test should be done by using UDP.

5. Test Scenario

This Chapter consists of following 4 sections of test scenarios.

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

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

Scope:

Following tests focus on Transport Mode.

Overview:

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

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

Purpose:

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

Category:

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

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

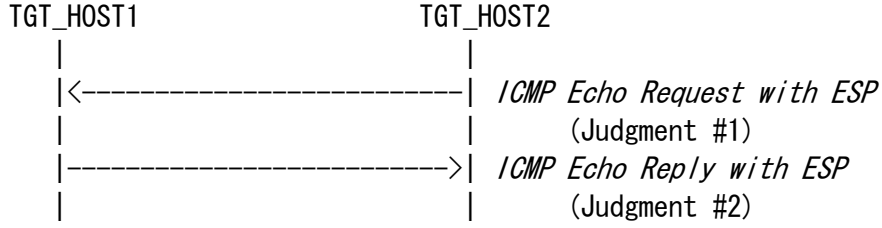
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC as an authentication algorithm)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

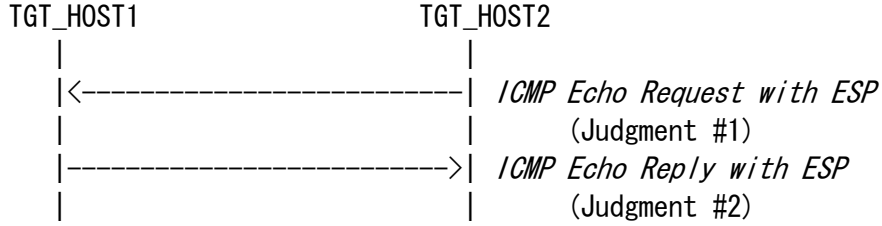
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc1to2
	Authentication Algorithm	AES-XCBC-MAC-96
	Authentication Key	ipv6readaesx1to2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

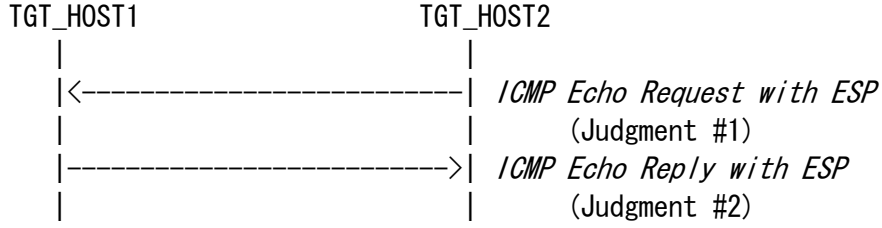
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

References:

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CBC(128-bit) as an encryption algorithm)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

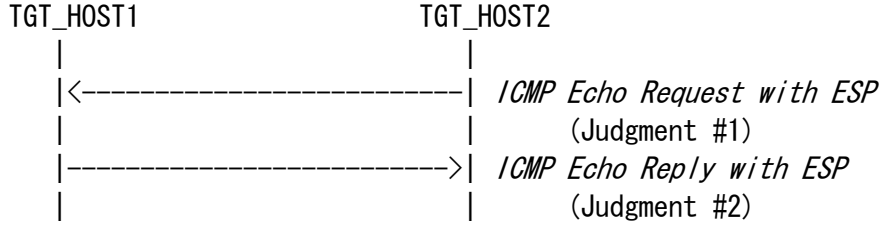
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

References:

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

RFC 2451: The ESP CBC-Mode Cipher Algorithms

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CTR as an encryption algorithm)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

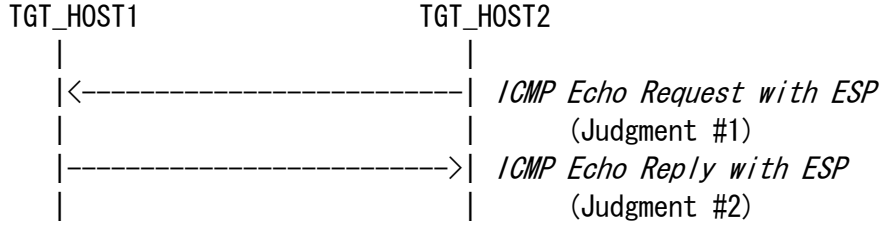
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	KEY	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

5.1.6. Transport Mode: ESP=NULL HMAC-SHA1

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support NULL as an encryption algorithm)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

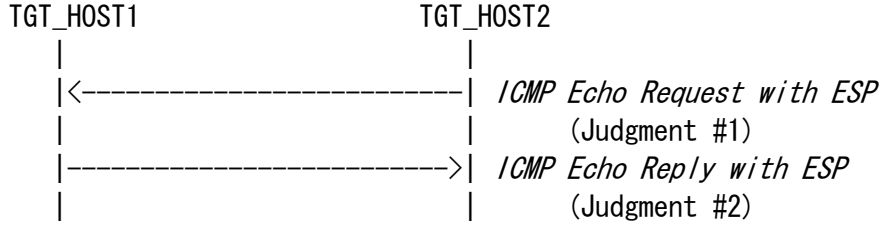
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support CAMELLIA-CBC(128-bit) as an encryption algorithm)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Transport
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

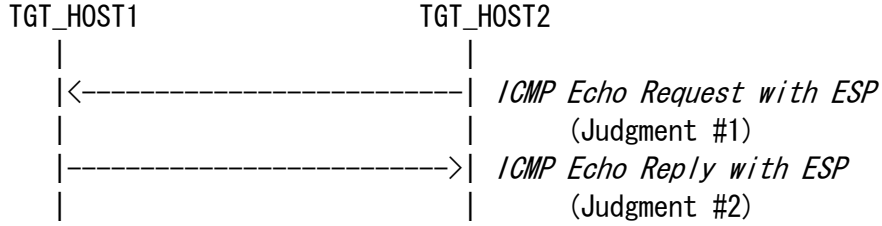
ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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 4312: The Camellia Cipher Algorithm and Its Use With IPsec

5.1.8. Transport Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that can select ICMP Type as SPD selector)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2  ---------------------  TGT_HOST1
   HOST2_SA1-O ---------------------> HOST1_SA1-I   ICMPv6 Echo Request
   HOST2_SA1-I <--------------------- HOST1_SA1-O   ICMPv6 Echo Request
   HOST2_SA2-O ---------------------> HOST1_SA2-I   ICMPv6 Echo Reply
   HOST2_SA2-I <--------------------- HOST1_SA2-O   ICMPv6 Echo Reply
```

Security Association Database (SAD) for HOST1_SA1-I

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

Security Policy Database (SPD) for HOST1_SA1-I

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

Security Association Database (SAD) for HOST1_SA1-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST1_SA1-O

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

Security Association Database (SAD) for HOST2_SA1-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST2_SA1-I

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

Security Association Database (SAD) for HOST2_SA1-O

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

Security Policy Database (SPD) for TGT_HOST2_SA1-O

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

Security Association Database (SAD) for HOST1_SA2-I

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

Security Policy Database (SPD) for HOST1_SA2-I

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

Security Association Database (SAD) for HOST1_SA2-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST1_SA2-O

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

Security Association Database (SAD) for HOST2_SA2-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST2_SA2-I

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

Security Association Database (SAD) for HOST2_SA2-O

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

Security Policy Database (SPD) for TGT_HOST2_SA2-O

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

Packets:

ICMP Echo Request with ESP1

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with ESP1

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

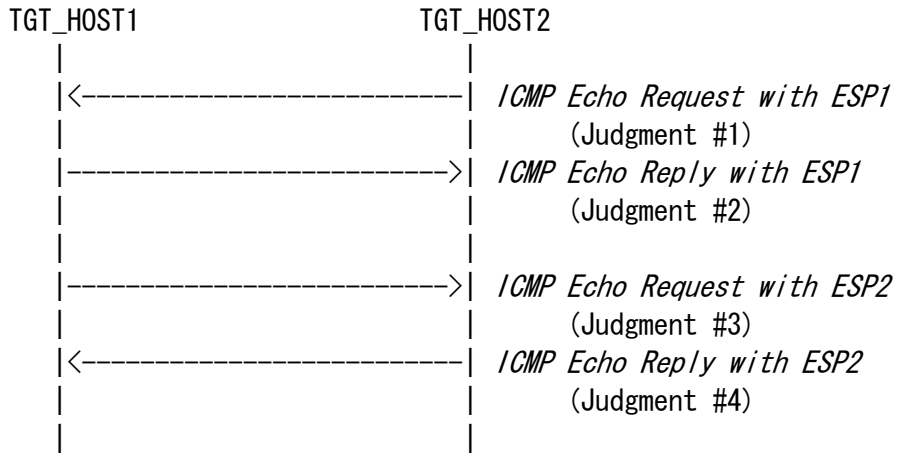
ICMP Echo Request with ESP2

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

ICMP Echo Reply with ESP2

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

Procedure:



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

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll and can skip step from 6 to 10.
If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

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

References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4443: Internet Control Message Protocol (ICMPv6)
for the Internet Protocol Version 6 (IPv6) Specification

5.1.9. Transport Mode: dummy packet handling

Purpose:

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

Category:

End-Node: ADVANCED (A requirement for all End-Node NUTs
that support dummy packet handling)
SGW : N/A

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ----------------------  TGT_HOST1
   HOST2_SA-O ---------------------> HOST1_SA-I
   HOST2_SA-I <--------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

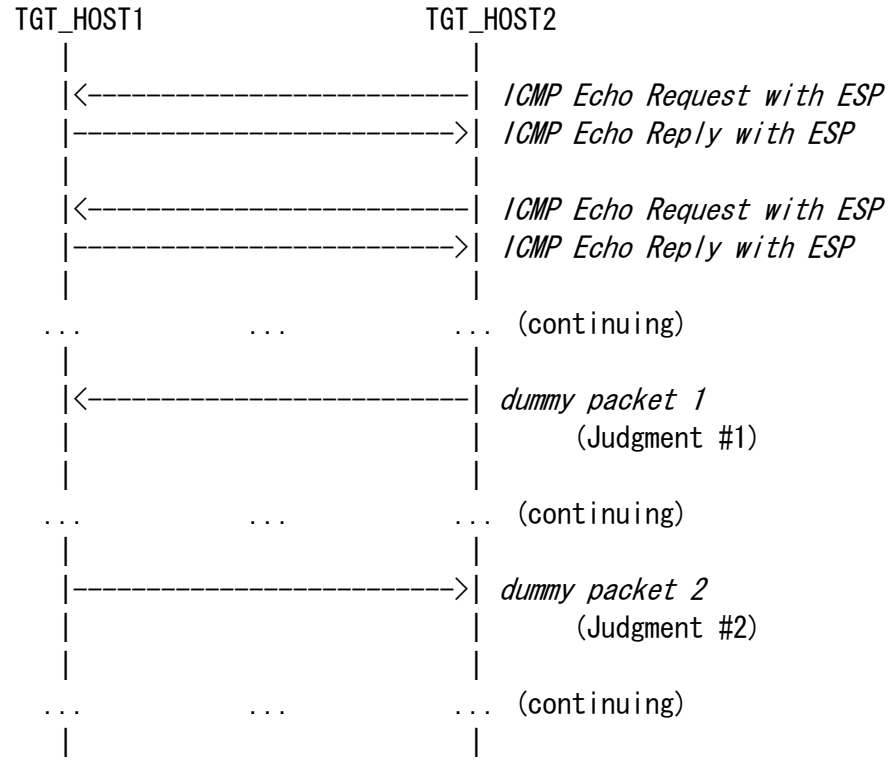
dummy packet 1

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

dummy packet 2

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"dummy packet 1"*
Judgment #2
  Step-3: TGT_HOST1 transmits *"dummy packet 2*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.1.10. Transport Mode: TFC padding

Purpose:

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

Category:

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

Initialization:

Use common topology described as Fig.1

Set NUT's SAD and SPD as following:

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ---------------------> HOST1_SA-I
   HOST2_SA-I <--------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for TGT_HOST2_SA-O

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

Packets:

ICMP Echo Request with ESP

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

ICMP Echo Reply with ESP

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

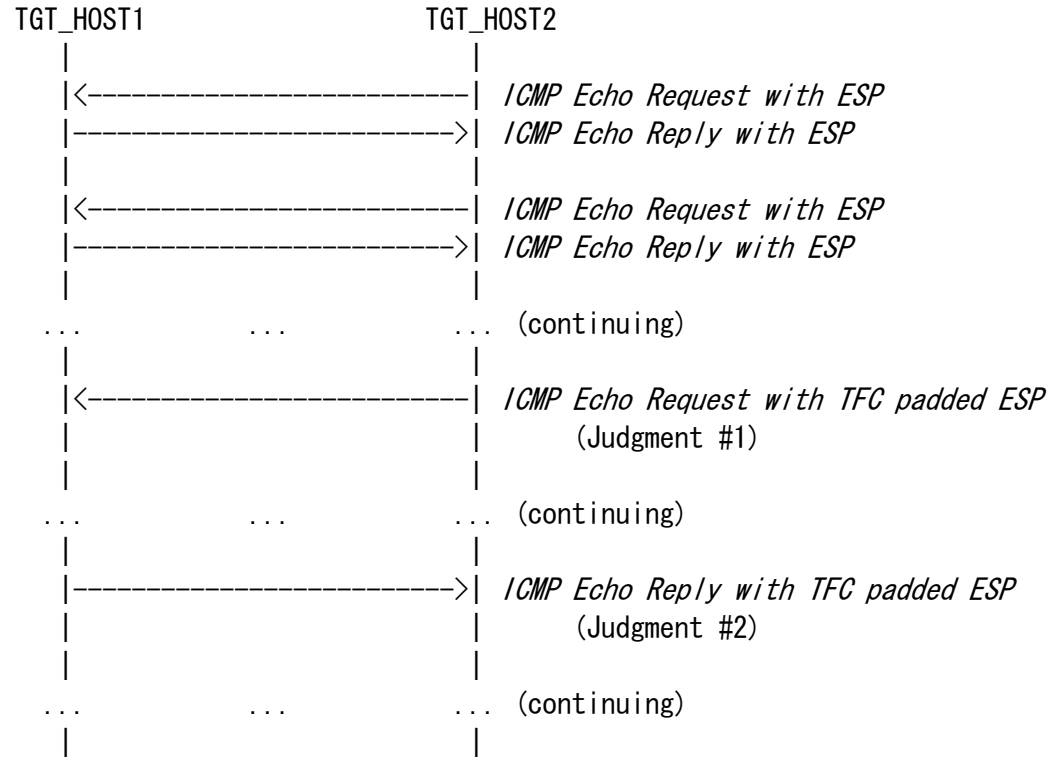
ICMP Echo Request with TFC padded ESP

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	KEY	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
ICMP	Type	128 (Echo Request)

ICMP Echo Reply with TFC padded ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with TFC padded ESP"*
Judgment #2
  Step-3: TGT_HOST1 transmits *"ICMP Echo Reply with TFC padded ESP"*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.2. Tunnel Mode (SGW vs. SGW)

Scope:

Following tests focus on Tunnel Mode between SGW and SGW.

Overview:

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

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

Purpose:

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

Category:

End-Node : N/A
SGW : BASIC (A requirement for all SGW NUTs if you choose SGW vs. SGW Tunnel mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

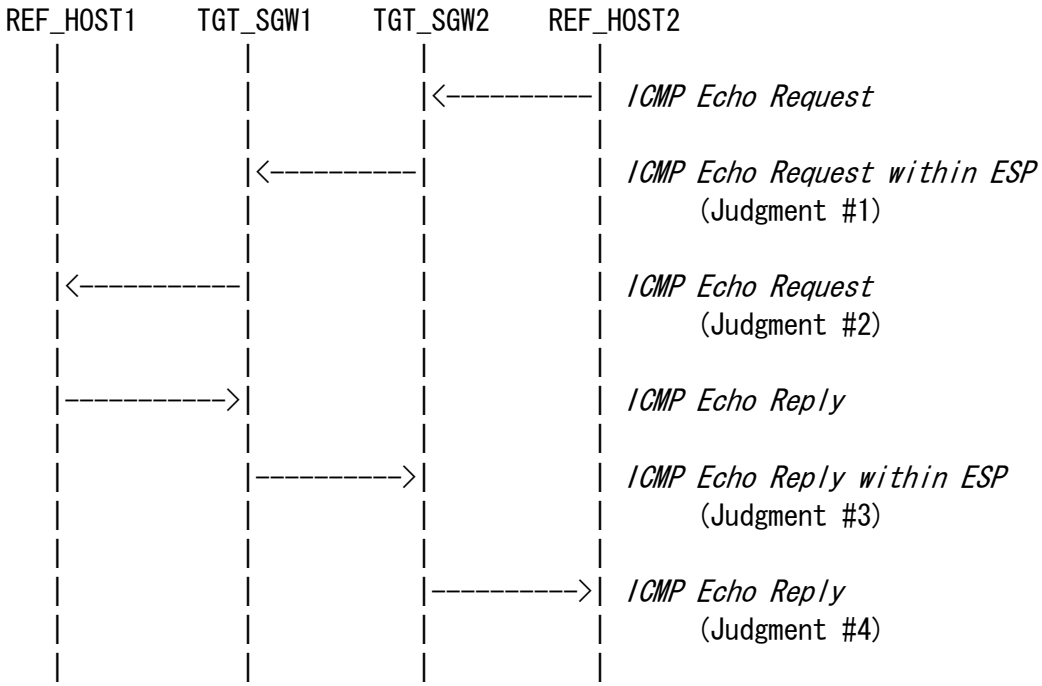
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

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)

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

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-XCBC as an authentication algorithm if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_SGW2_Link2
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx2to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

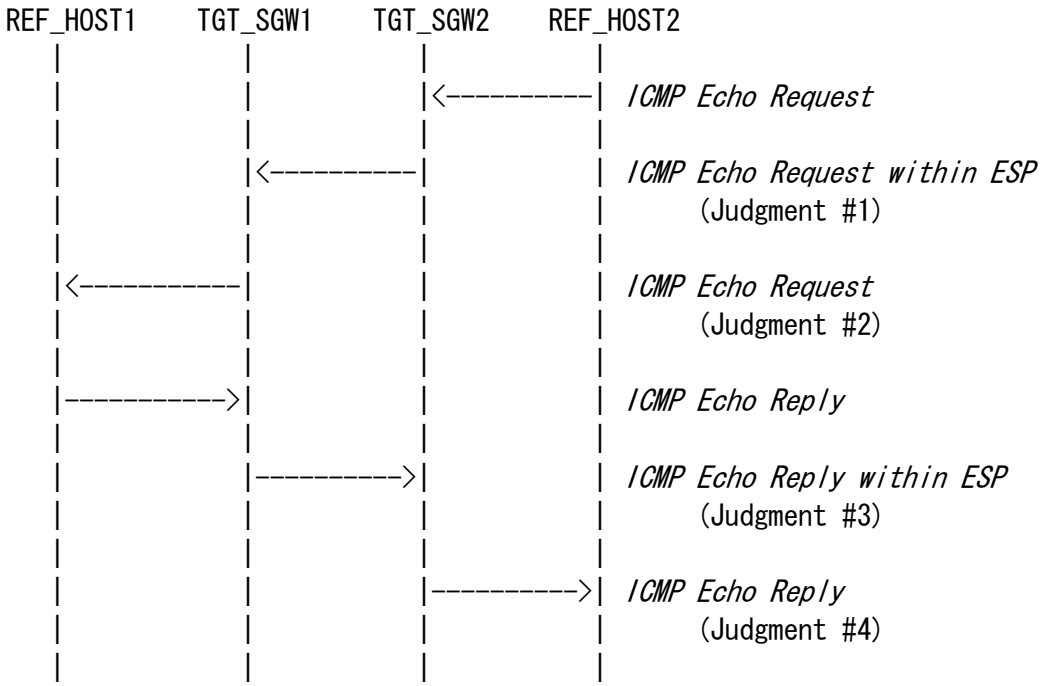
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

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)

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

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an authentication algorithm if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	NULL
	Authentication Key	
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

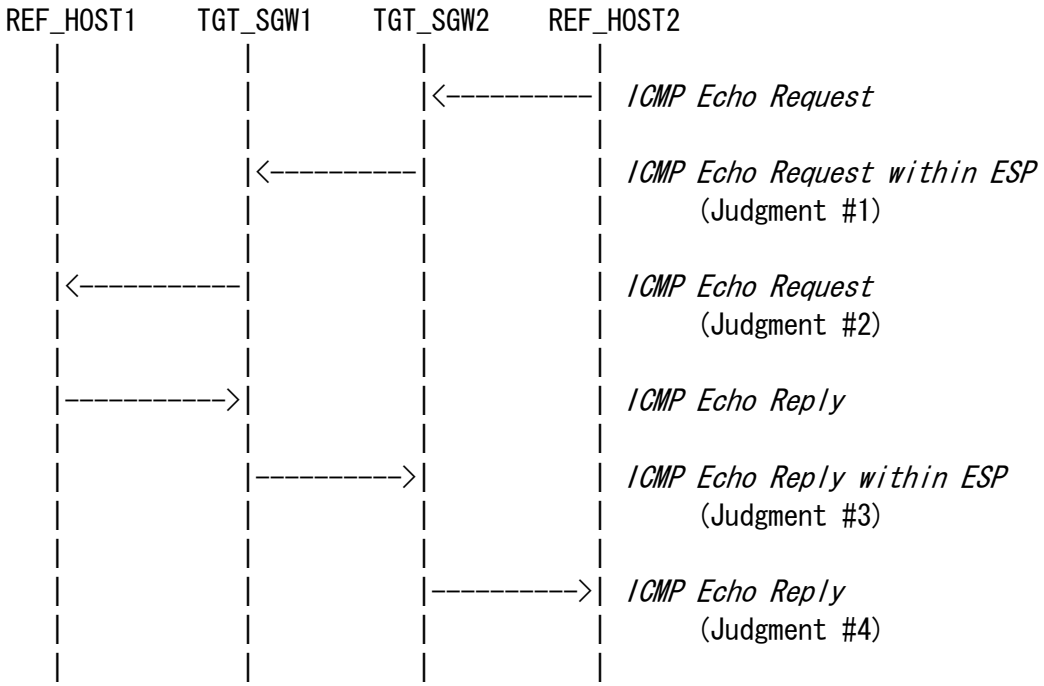
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

References:

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)

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

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CBC(128-bit) as an encryption algorithm if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaesc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

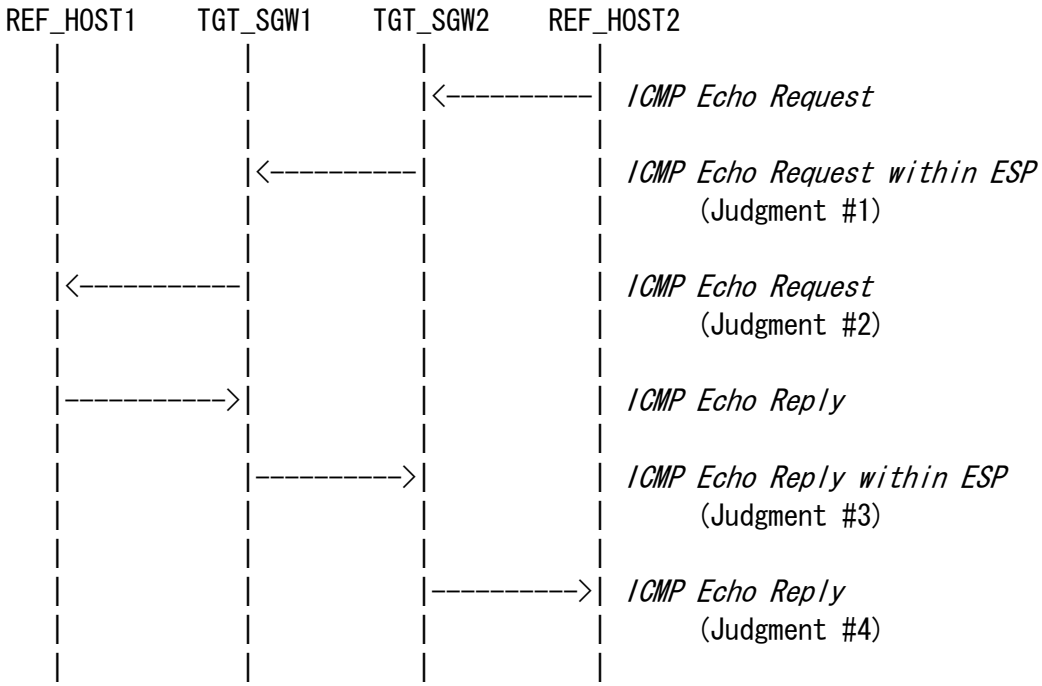
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

References:

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

RFC 2451: The ESP CBC-Mode Cipher Algorithms

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)

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

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CTR as an encryption algorithm if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

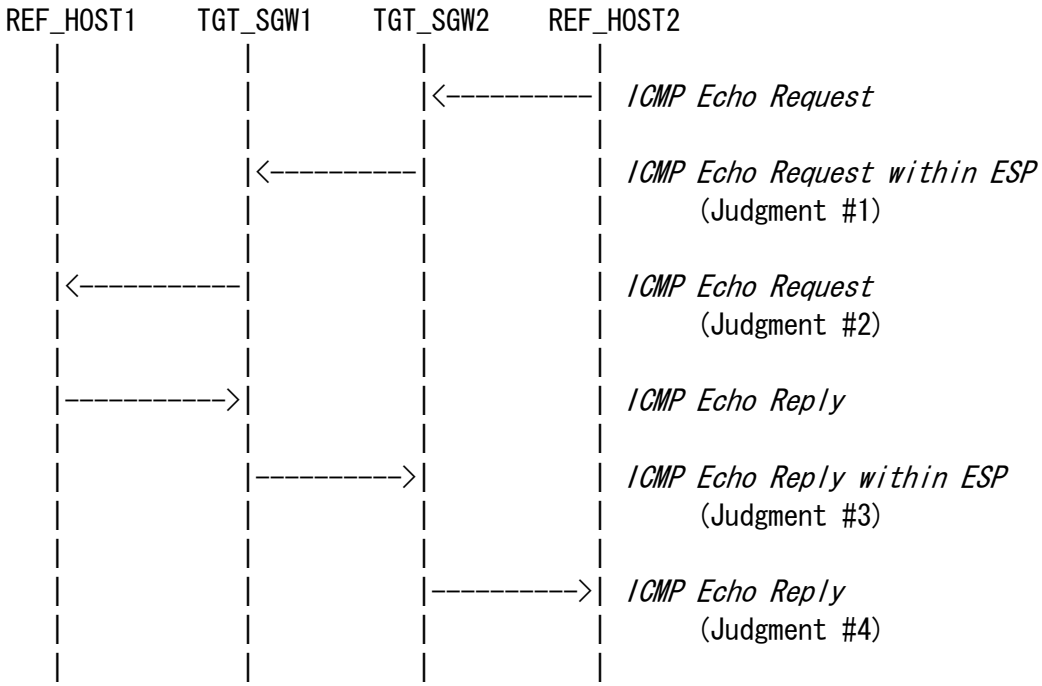
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

IP Header	Source Address	TGT_SGW1_Link1
	Destination Address	TGT_SGW2_Link2
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

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)

5.2.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an encryption algorithm are required to satisfy if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

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

ICMP Echo Request

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

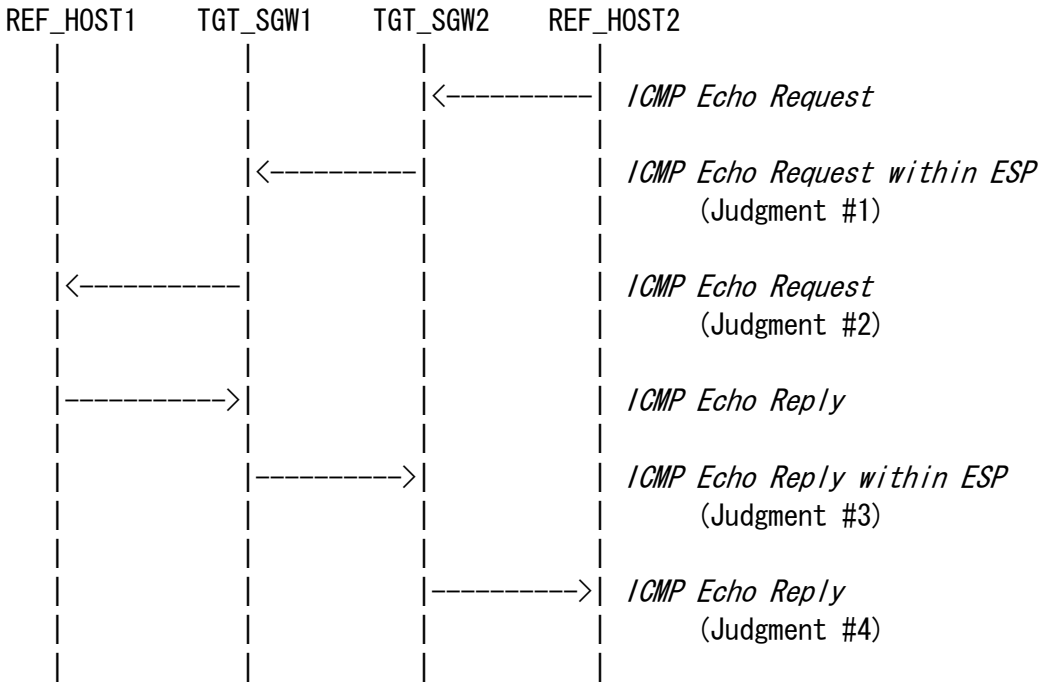
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

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)

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

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose SGW vs. SGW Tunnel Mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
Mode	tunnel
Protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP key	ipv6readcamc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	CAMELLILA-CBC(128-bit)
	Key	ipv6readcamc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

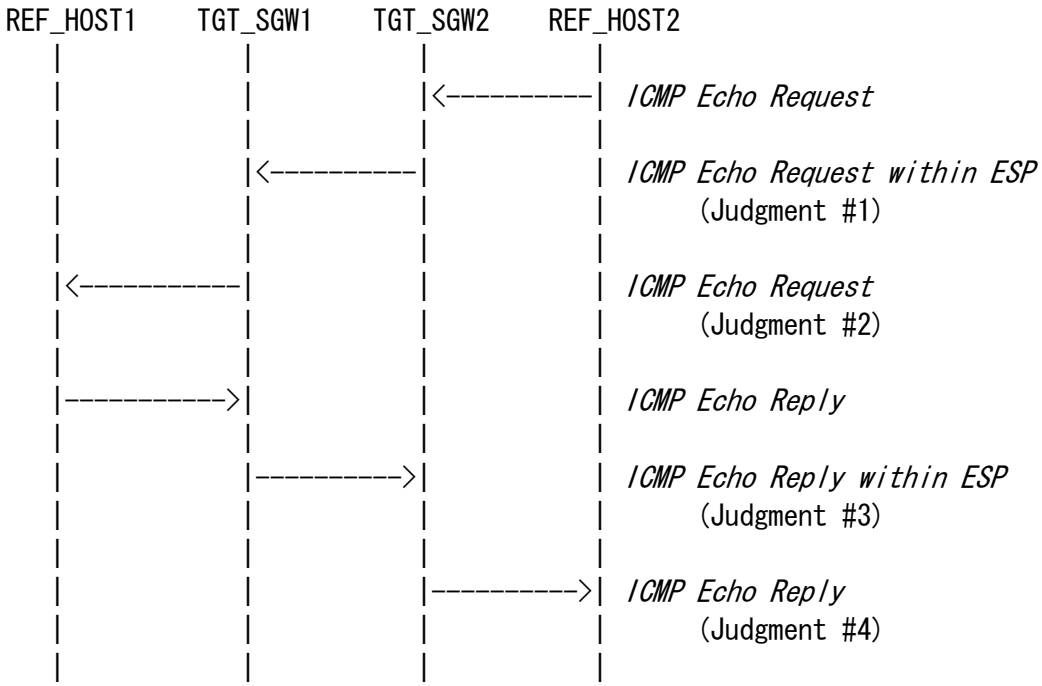
ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Request"*
Judgment #3
  Step-4: TGT_SGW1 transmits *"ICMP Echo Reply within ESP"*
Judgment #4
  Step-5: TGT_SGW2 transmits *"ICMP Echo Reply"*

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 4312: The Camellia Cipher Algorithm and Its Use With IPsec

5.2.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that can select ICMP Type as SPD selector, if you choose SGW vs. SGW Tunnel mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ---------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA1-O ------------------> SGW1_SA1-I  ICMPv6 Echo Request
             SGW2_SA1-I <------------------ SGW1_SA1-O  ICMPv6 Echo Request
             SGW2_SA2-O ------------------> SGW1_SA2-I  ICMPv6 Echo Reply
             SGW2_SA2-I <------------------ SGW1_SA2-O  ICMPv6 Echo Reply
```

Security Association Database (SAD) for SGW1_SA1-I

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1req

Security Policy Database (SPD) for SGW1_SA1-I

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

Security Association Database (SAD) for SGW1_SA1-O

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

Security Policy Database (SPD) for SGW1_SA1-O

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

Security Association Database (SAD) for SGW2_SA1-I

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

Security Policy Database (SPD) for SGW2_SA1-I

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

Security Association Database (SAD) for SGW2_SA1-O

source address	TGT_SGW2_Link2
destination address	TGT_SGW1_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	ipv6readylogo3des2to1req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha12to1req

Security Policy Database (SPD) for SGW2_SA1-O

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

Security Association Database (SAD) for SGW1_SA2-I

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

Security Policy Database (SPD) for SGW1_SA2-I

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

Security Association Database (SAD) for SGW1_SA2-O

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

Security Policy Database (SPD) for SGW1_SA2-O

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

Security Association Database (SAD) for SGW2_SA2-I

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

Security Policy Database (SPD) for SGW2_SA2-I

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

Security Association Database (SAD) for SGW2_SA2-O

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

Security Policy Database (SPD) for SGW2_SA2-O

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

Packets:

ICMP Echo Request1 within ESP1

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1req
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request1

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

ICMP Echo Reply1

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply1 within ESP1

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

ICMP Echo Request2 within ESP2

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

ICMP Echo Request2

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

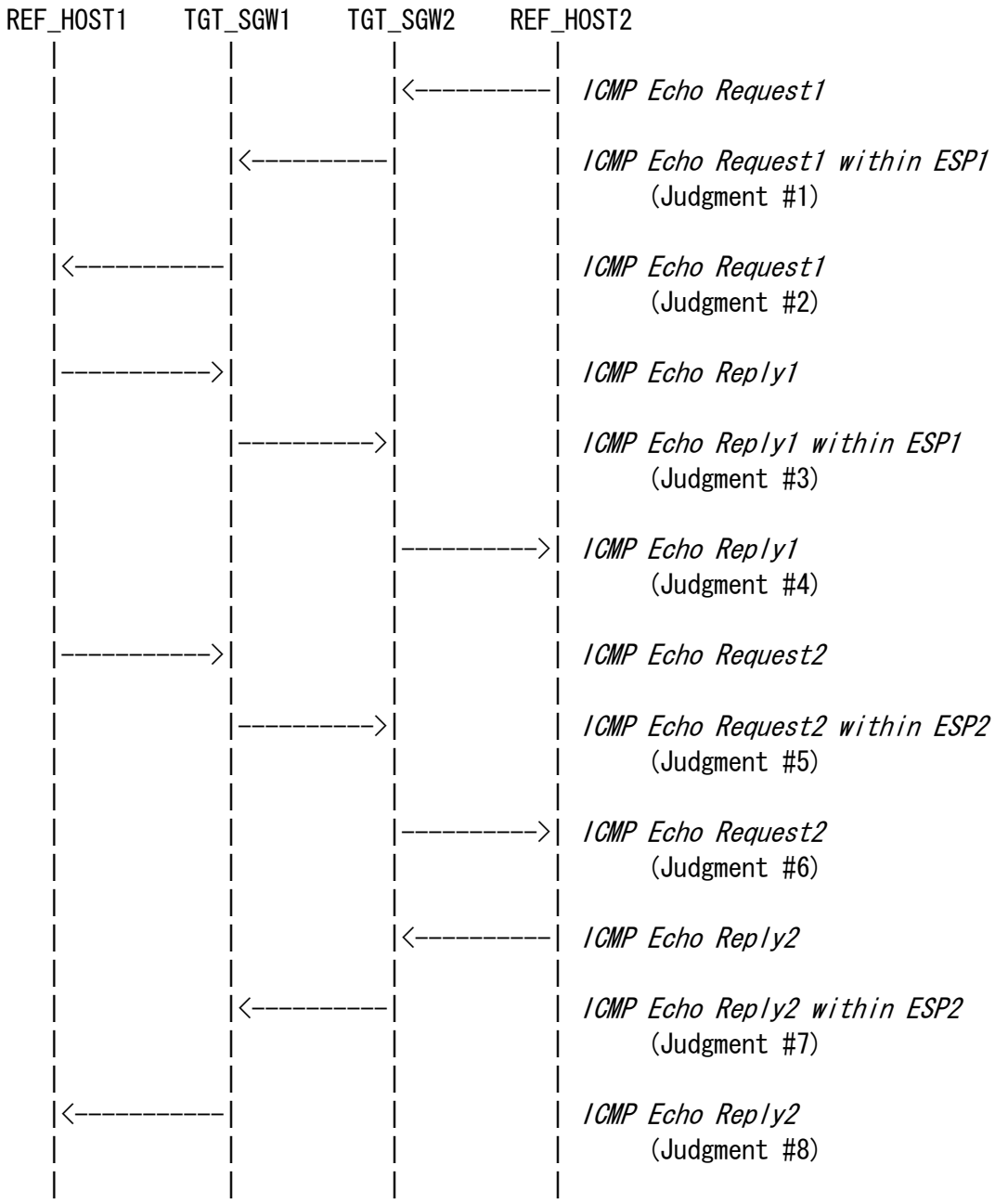
ICMP Echo Reply2

IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply2 within ESP2

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

Procedure:


REF_HOST1
TGT_SGW1
TGT_SGW2
REF_HOST2
ICMP Echo Request1
ICMP Echo Request1 within ESP1
(Judgment #1)
ICMP Echo Request1
(Judgment #2)
ICMP Echo Reply1
ICMP Echo Reply1 within ESP1
(Judgment #3)
ICMP Echo Reply1
(Judgment #4)
ICMP Echo Request2
ICMP Echo Request2 within ESP2
(Judgment #5)
ICMP Echo Request2
(Judgment #6)
ICMP Echo Reply2
ICMP Echo Reply2 within ESP2
(Judgment #7)
ICMP Echo Reply2
(Judgment #8)

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

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

Judgment:

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

References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4443: Internet Control Message Protocol (ICMPv6)
for the Internet Protocol Version 6 (IPv6) Specification

5.2.9. Tunnel Mode: dummy packet handling

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support dummy packet handling if you choose SGW vs. SGW Tunnel mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

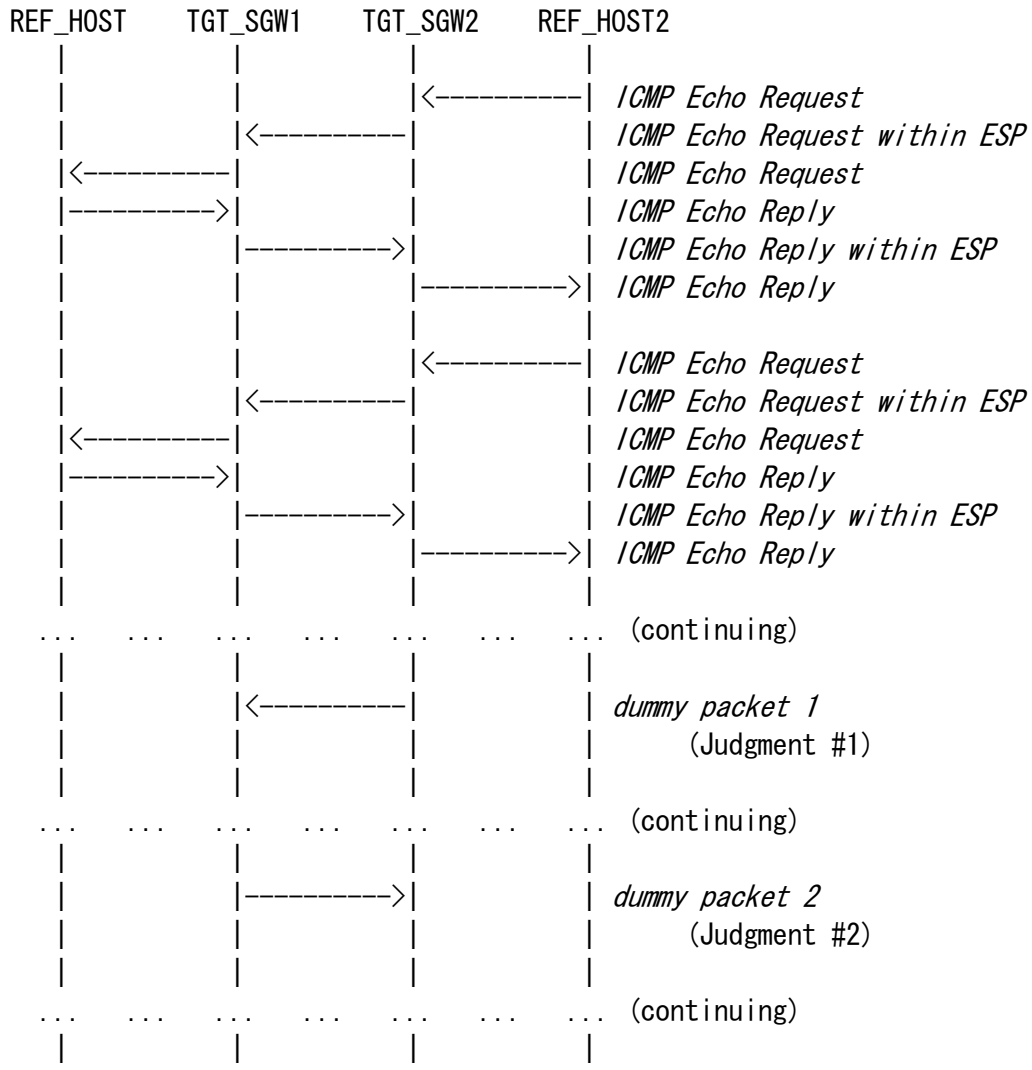
dummy packet 1

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

dummy packet 2

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"dummy packet 1"*
Judgment #3
  Step-3: TGT_SGW1 transmits *"dummy packet 2"*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.2.10. Tunnel Mode: TFC padding

Purpose:

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

Category:

End-Node : N/A
SGW : ADVANCED (A requirement for all SGW NUTs that support TFC padding handling if you choose SGW vs. SGW Tunnel mode)

Initialization:

Use common topology described as Fig.2

Set NUT's SAD and SPD as following:

```
REF_HOST2 -- TGT_SGW2 ------------------- TGT_SGW1 -- REF_HOST1
             SGW2_SA-O ------------------> SGW1_SA-I
             SGW2_SA-I <------------------ SGW1_SA-O
```

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for SGW2_SA-I

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

Security Policy Database (SPD) for SGW2_SA-I

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

Security Association Database (SAD) for SGW2_SA-O

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

Security Policy Database (SPD) for SGW2_SA-O

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

Packets:

ICMP Echo Request within ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request

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

ICMP Echo Reply

IP Header	Source Address	REF_HOST1_Link0
	Destination Address	REF_HOST2_Link3
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply within ESP

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

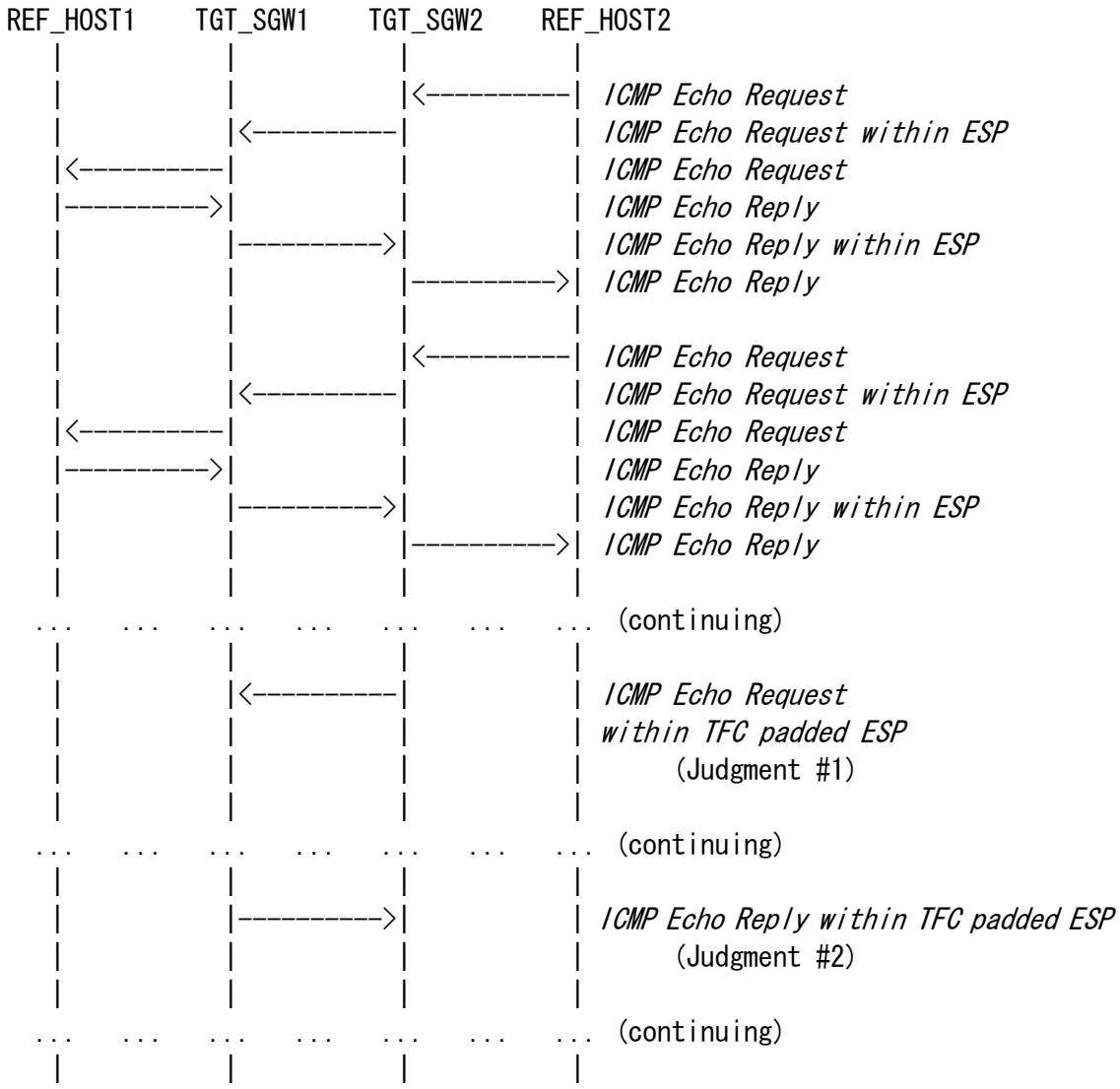
ICMP Echo Request within TFC padded ESP

IP Header	Source Address	TGT_SGW2_Link2
	Destination Address	TGT_SGW1_Link1
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
IP Header	Source Address	REF_HOST2_Link3
	Destination Address	REF_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within TFC padded ESP

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_SGW2 transmits *"ICMP Echo Request within TFC padded ESP"*
Judgment #2
  Step-3: TGT_SGW1 transmits *"ICMP Echo Reply within TFC padded ESP"*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

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

Scope:

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

Overview:

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

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

Purpose:

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

Category:

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

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

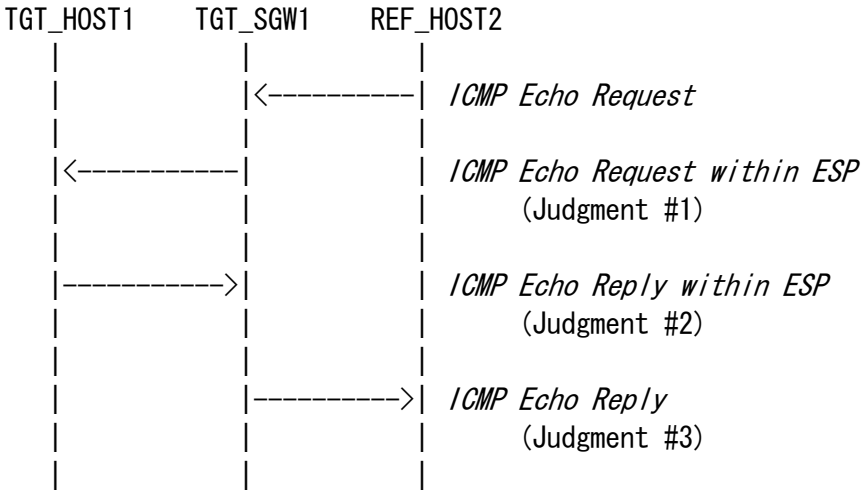
ICMP Echo Reply within ESP tunnel

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

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC as an authentication algorithm if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-XCBC as an authentication algorithm if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

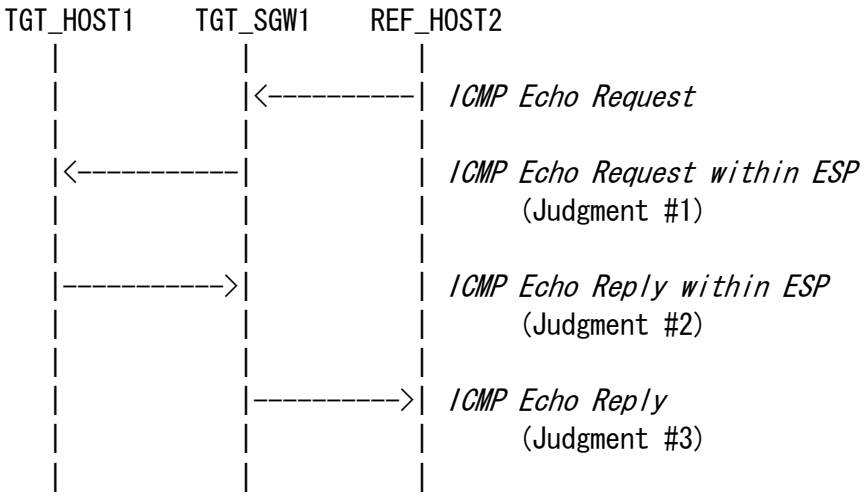
ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesxstoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support NULL as an authentication algorithm if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an authentication algorithm if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

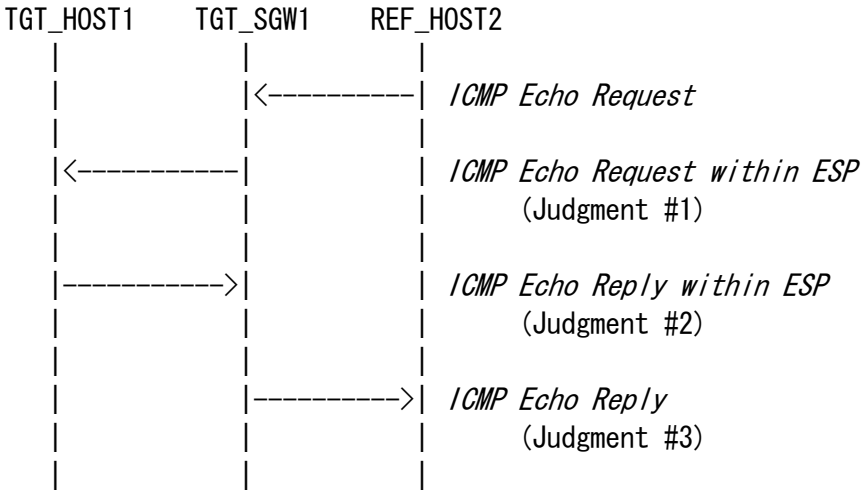
ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	NULL
	Authentication Key	
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

References:

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaescetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

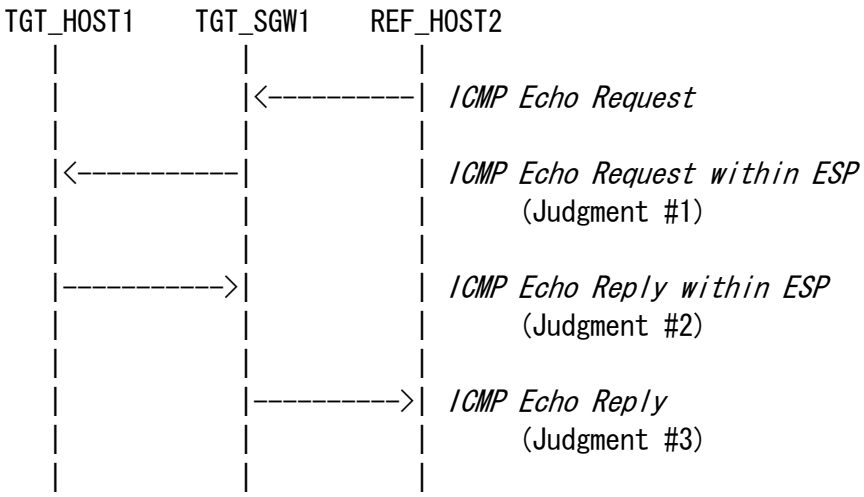
ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	AES-CBC(128-bit)
	Key	ipv6readaescstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

References:

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

RFC 2451: The ESP CBC-Mode Cipher Algorithms

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CTR as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support AES-CTR as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaesetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaesstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaesstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaesetos
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1etos

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

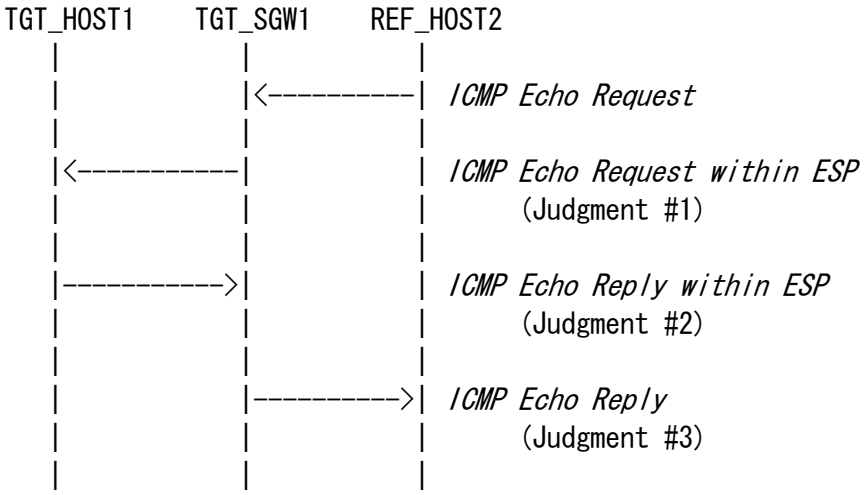
ICMP Echo Reply within ESP tunnel

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

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

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)

5.3.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support NULL as an encryption algorithm are required to satisfy if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support NULL as an encryption algorithm are required to satisfy if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

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

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

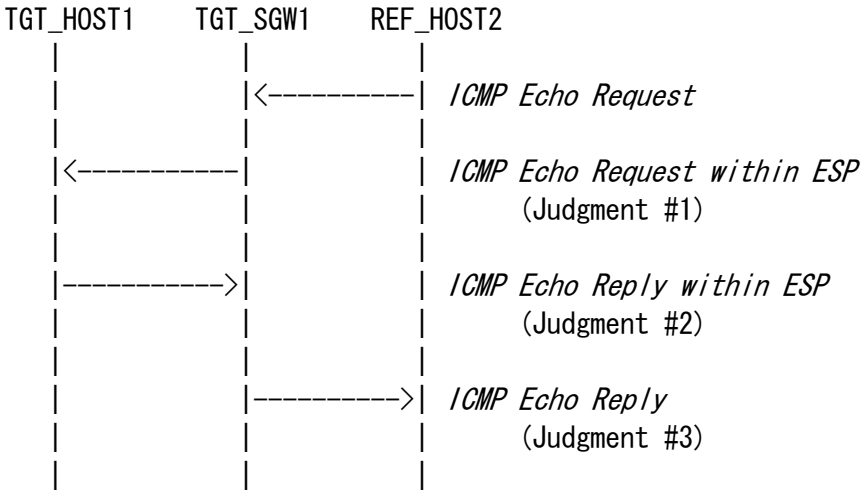
ICMP Echo Reply within ESP tunnel

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

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	Any
direction	In
protocol	ESP
mode	Tunnel

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_HOST2_Link2
destination address	TGT_HOST1_Link0
upper spec	Any
direction	In
protocol	ESP
mode	Tunnel

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

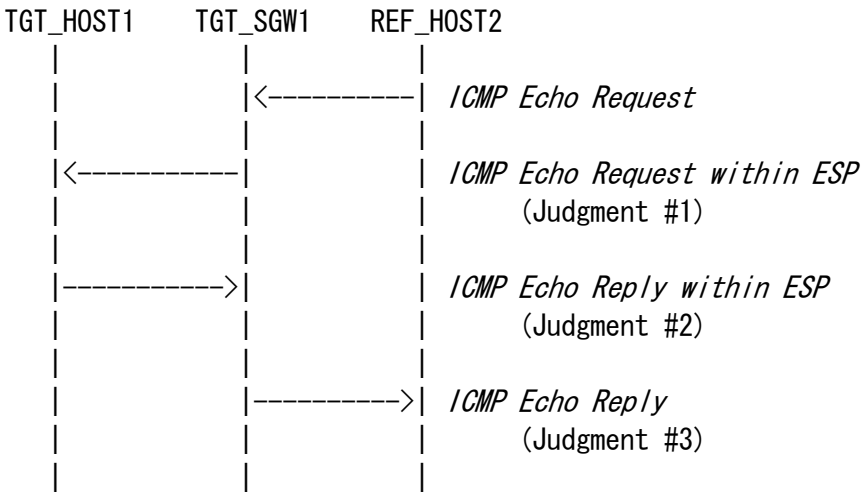
ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	CAMELLIA-CBC(128-bit)
	Key	ipv6readcamcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within ESP tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply"*.

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 4312: The Camellia Cipher Algorithm and Its Use With IPsec

5.3.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that can select ICMP Type as SPD selector if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that can select ICMP Type as SPD selector if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA1-I

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

Security Policy Database (SPD) for SGW1_SA1-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA1-O

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

Security Policy Database (SPD) for SGW1_SA1-O

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_HOST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA1-I

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

Security Policy Database (SPD) for HOST1_SA1-I

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_HOST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Request
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA1-O

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

Security Policy Database (SPD) for HOST1_SA1-O

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	ICMPv6 Echo Request
direction	Out
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA2-I

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3desetosrep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1etosrep

Security Policy Database (SPD) for SGW1_SA2-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SGW1_SA2-O

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

Security Policy Database (SPD) for SGW1_SA2-O

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_HOST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA2-I

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

Security Policy Database (SPD) for HOST1_SA2-I

tunnel source address	TGT_SGW1_Link1
tunnel destination address	TGT_HOST1_Link0
source address	REF_HOST2_Link2
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA2-O

source address	TGT_HOST1_Link0
destination address	TGT_SGW1_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3desetosrep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha1etosrep

Security Policy Database (SPD) for HOST1_SA2-O

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_SGW1_Link1
source address	TGT_HOST1_Link0
destination address	REF_HOST2_Link2
upper spec	ICMPv6 Echo Reply
direction	Out
protocol	ESP
mode	tunnel

Packets:

ICMP Echo Request1

IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request1 within ESP1 tunnel

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desstoereq
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1stoereq
IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply1 within ESP1 tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desetosrep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosrep
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply1

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

ICMP Echo Request2 within ESP2 tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3desetosreq
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha1etosreq
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	128 (Echo Request)

ICMP Echo Request2

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	128 (Echo Request)

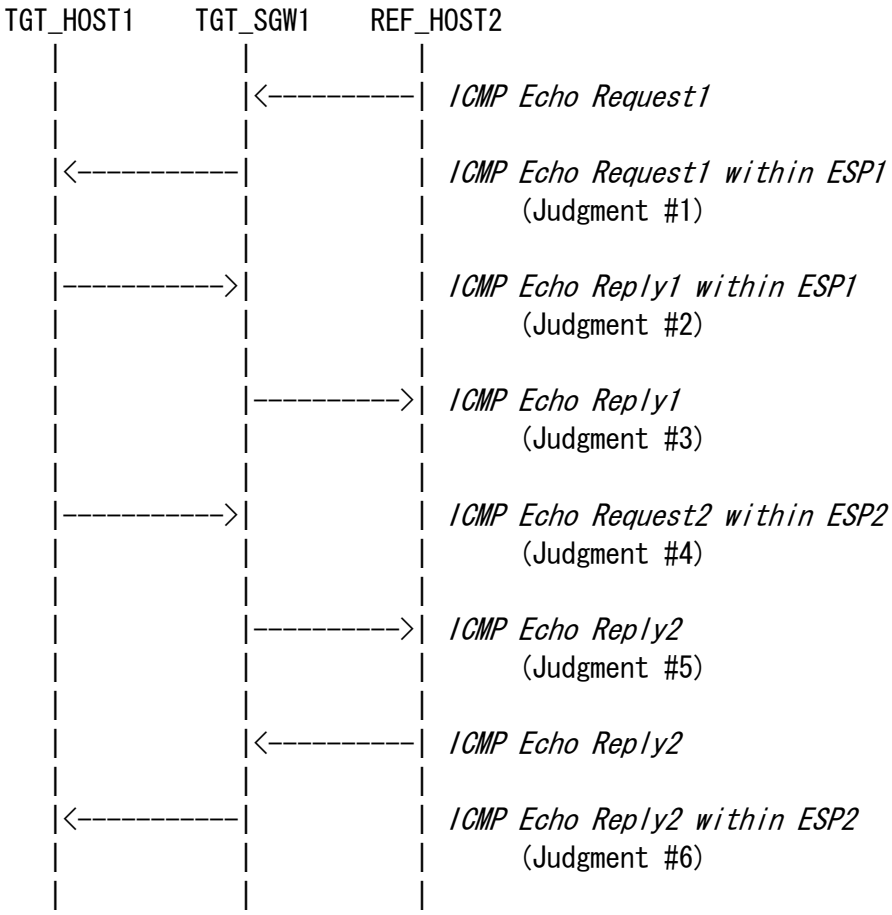
ICMP Echo Reply2

IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	129 (Echo Reply)

ICMP Echo Reply2 within ESP2 tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request1 within ESP1 tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply1 within ESP1 tunnel"*.
Judgment #3
  Step-4: TGT-SGW1 transmits the packet *"ICMP Echo Reply1"*.
Judgment #4
  Step-7: TGT-HOST1 transmits the packet *"ICMP Echo Request2 within ESP2 tunnel"*.
Judgment #5
  Step-8: TGT-SGW1 transmits the packet *"ICMP Echo Request2 "*.
Judgment #6
  Step-9: TGT-SGW1 transmits the packet *"ICMP Echo Reply within ESP2 tunnel"*.

References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4443: Internet Control Message Protocol (ICMPv6)
for the Internet Protocol Version 6 (IPv6) Specification

5.3.9. Tunnel Mode: dummy packet handling

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support dummy packet handling if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support dummy packet handling if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request

IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

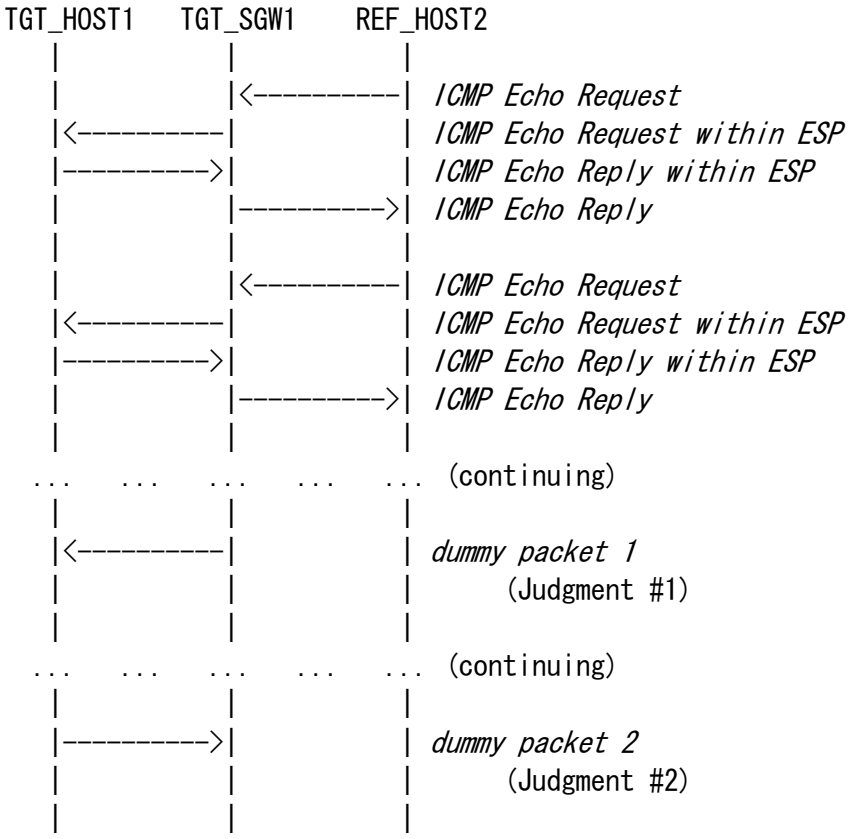
dummy packet 1

IP Header	Source Address	TGT_SGW_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcetos
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1etos
	Next Header	59 (no next header)

dummy packet 2

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"dummy packet 1"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"dummy packet 2"*.

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.3.10. Tunnel Mode: TFC padding

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support TFC padding if you choose End-Node vs. SGW Tunnel Mode)
SGW : ADVANCED (A requirement for all SGW NUTs that support TFC padding if you choose End-Node vs. SGW Tunnel Mode)

Initialization:

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

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

Security Association Database (SAD) for SGW1_SA-I

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

Security Policy Database (SPD) for SGW1_SA-I

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

Security Association Database (SAD) for SGW1_SA-O

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for SGW1_SA-O

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

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_SGW1_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbcstoe
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha1stoe

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Packets:

ICMP Echo Request

IP Header	Source Address	REF_HOST2_Link2
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

ICMP Echo Reply

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

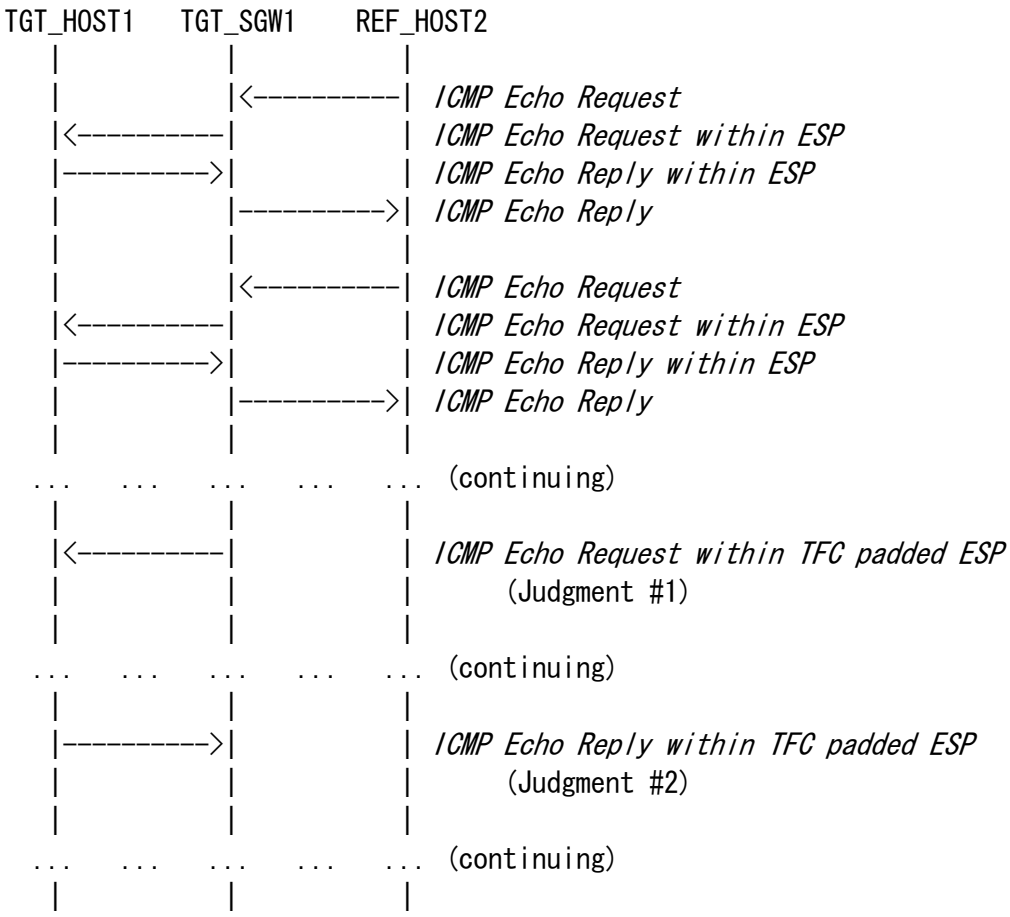
ICMP Echo Request within TFC padded ESP tunnel

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

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_SGW_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbcstoe
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha1stoe
	TFC padding	any size other than 0 byte
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	REF_HOST2_Link2
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT-SGW1 transmits the packet *"ICMP Echo Request within TFC padded ESP tunnel"*.
Judgment #2
  Step-3: TGT-HOST1 transmits the packet *"ICMP Echo Reply within TFC padded ESP tunnel"*.

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.4. Tunnel Mode (End-Node vs. End-Node)

Scope:

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

Overview:

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

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

Purpose:

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

Category:

End-Node : BASIC (A requirement for all End-Node NUTs if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

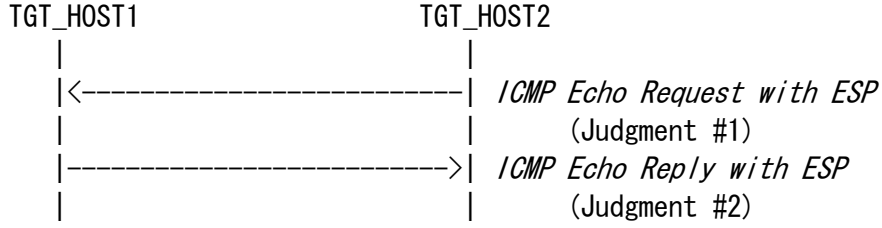
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-XCBC as an authentication algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx1to2

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	AES-XCBC
ESP authentication key	ipv6readaesx2to1

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

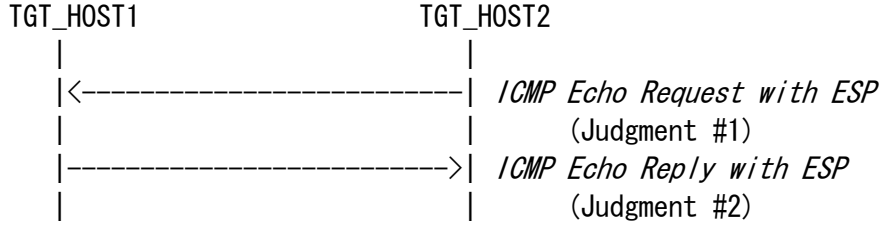
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc1to2
	Authentication Algorithm	AES-XCBC
	Authentication Key	ipv6readaesx1to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support NULL as an authentication algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc1to2
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3descbc2to1
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

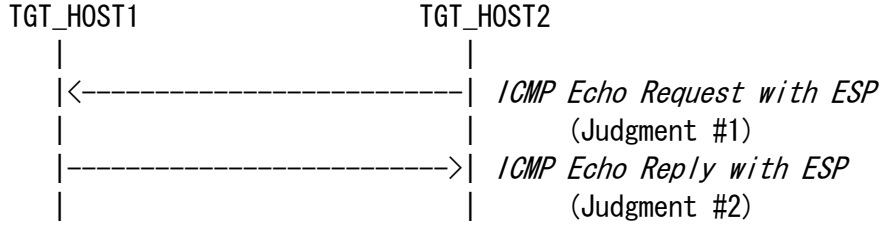
ICMP Echo Request within ESP tunnel

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	NULL
	Authentication Key	
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

References:

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC(128-bit)
ESP algorithm key	ipv6readaesc2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

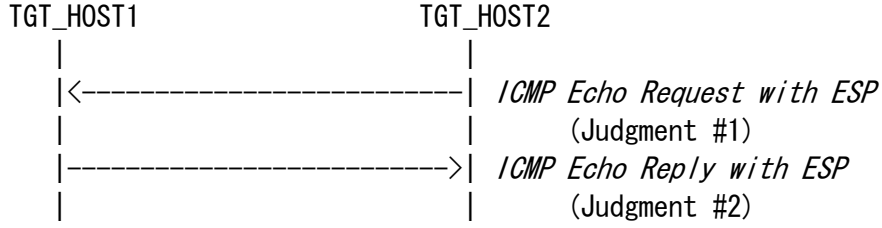
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

References:

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

RFC 2451: The ESP CBC-Mode Cipher Algorithms

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support AES-CTR as an encryption algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CTR
ESP algorithm key	ipv6readylogoaes2to1
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha12to1

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

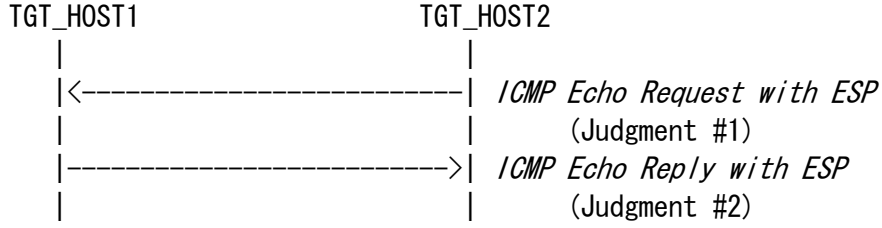
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x2000
	Algorithm	AES-CTR
	Key	ipv6readylogoaes1to2
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha11to2
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

5.4.6. Tunnel Mode: ESP=NULL HMAC-SHA1

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support NULL as an encryption algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

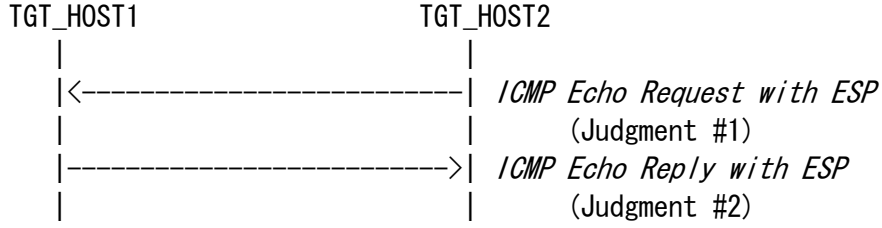
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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)

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

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support CAMELLIA-CBC(128-bit) as an encryption algorithm if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
   HOST2_SA-O ----------------------> HOST1_SA-I
   HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	Tunnel
protocol	ESP
ESP algorithm	CAMELLIA-CBC(128-bit)
ESP algorithm key	ipv6readcamc1to2
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readylogsha11to2

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

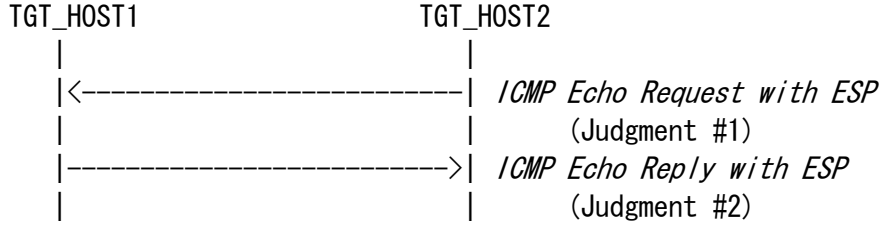
ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with ESP"*
Judgment #2
  Step-4: TGT_HOST1 transmits *"ICMP Echo Reply with ESP"*

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 4312: The Camellia Cipher Algorithm and Its Use With IPsec

5.4.8. Tunnel Mode: Select SPD (ICMP Type)

Purpose:

Selecting ICMP Type as SPD selector

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that can select ICMP Type as SPD selector if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2  --------------------   TGT_HOST1
   HOST2_SA1-O ---------------------> HOST1_SA1-I   ICMPv6 Echo Request
   HOST2_SA1-I <--------------------- HOST1_SA1-O   ICMPv6 Echo Request
   HOST2_SA2-O ---------------------> HOST1_SA2-I   ICMPv6 Echo Reply
   HOST2_SA2-I <--------------------- HOST1_SA2-O   ICMPv6 Echo Reply
```

Security Association Database (SAD) for HOST1_SA1-I

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

Security Policy Database (SPD) for HOST1_SA1-I

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

Security Association Database (SAD) for HOST1_SA1-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST1_SA1-O

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

Security Association Database (SAD) for HOST2_SA1-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2req
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2req

Security Policy Database (SPD) for HOST2_SA1-I

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

Security Association Database (SAD) for HOST2_SA1-O

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

Security Policy Database (SPD) for HOST2_SA1-O

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

Security Association Database (SAD) for HOST1_SA2-I

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

Security Policy Database (SPD) for HOST1_SA2-I

tunnel source address	TGT_HOST2_Link1
tunnel destination address	TGT_HOST1_Link0
source address	TGT_HOST2_Link1
destination address	TGT_HOST1_Link0
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST1_SA2-O

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST1_SA2-O

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

Security Association Database (SAD) for HOST2_SA2-I

source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
SPI	0x4000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP algorithm key	ipv6readylogo3des1to2rep
ESP authentication	HMAC-SHA1
ESP authentication key	ipv6readysha11to2rep

Security Policy Database (SPD) for HOST2_SA2-I

tunnel source address	TGT_HOST1_Link0
tunnel destination address	TGT_HOST2_Link1
source address	TGT_HOST1_Link0
destination address	TGT_HOST2_Link1
upper spec	ICMPv6 Echo Reply
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for HOST2_SA2-O

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

Security Policy Database (SPD) for HOST2_SA2-O

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

Packets:

ICMP Echo Request within ESP1 tunnel

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des2to1req
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha12to1req
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within ESP1 tunnel

IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ESP	SPI	0x4000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3des1to2rep
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readysha11to2rep
IP Header	Source Address	TGT_HOST1_Link0
	Destination Address	TGT_HOST2_Link1
ICMP	Type	129 (Echo Reply)

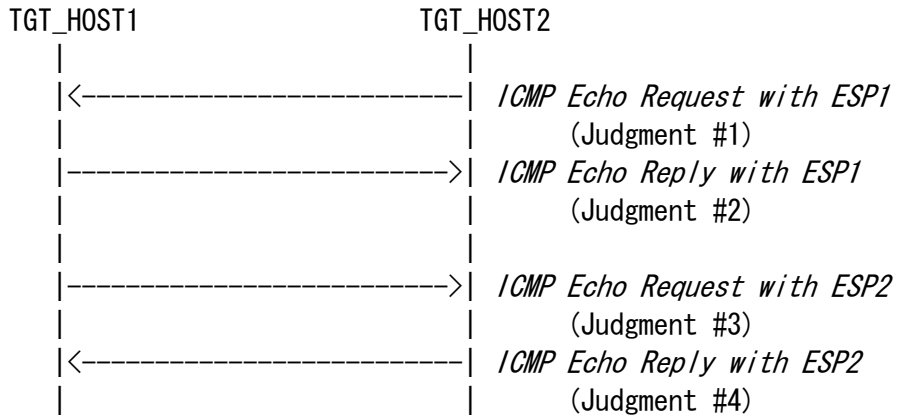
ICMP Echo Request within ESP2 tunnel

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

ICMP Echo Reply within ESP2 tunnel

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

Procedure:



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

NOTE: If your device can not send ICMP Echo Request, it must play TGT_HOST1 roll and can skip step from 6 to 10.
If your device can send ICMP Echo Request, it can play either TGT_HOST1 or TGT_HOST2. In either case choose a device which can send ICMP Echo Request as TGT_HOST2.

Judgment:

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

References:

RFC 4301: Security Architecture for the Internet Protocol

RFC 4303: IP Encapsulating Security Payload (ESP)

RFC 4443: Internet Control Message Protocol (ICMPv6)
for the Internet Protocol Version 6 (IPv6) Specification

5.4.9. Tunnel Mode: dummy packet handling

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support dummy packet handling if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ---------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

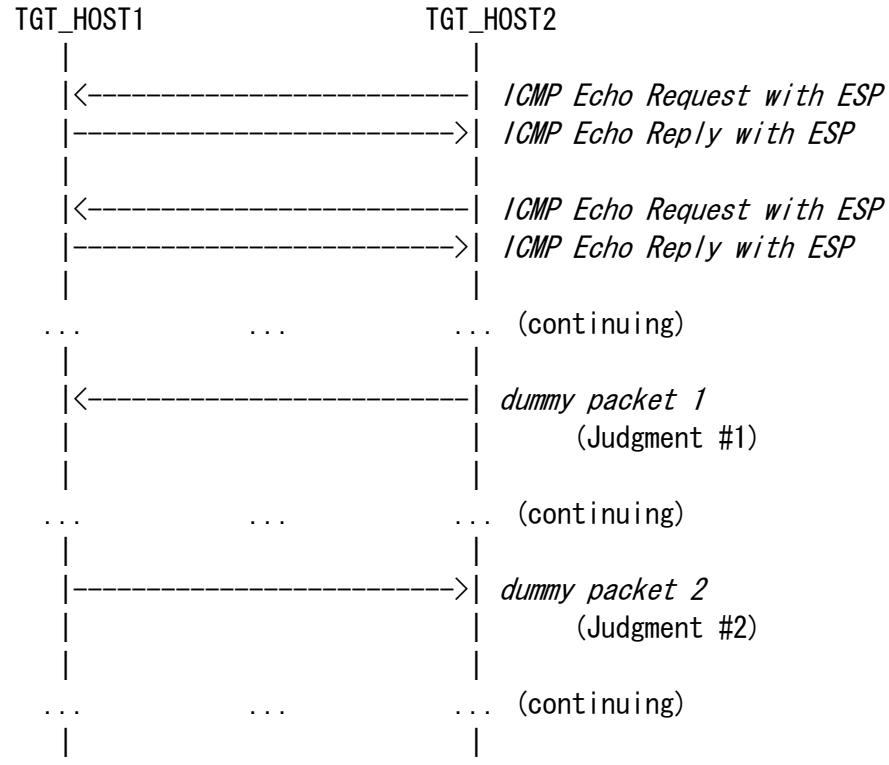
dummy packet 1

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

dummy packet 2

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"dummy packet 1"*
Judgment #2
  Step-3: TGT_HOST1 transmits *"dummy packet 2"*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

5.4.10. Tunnel Mode: TFC padding

Purpose:

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

Category:

End-Node : ADVANCED (A requirement for all End-Node NUTs that support TFC padding
if you choose End-Node vs. End-Node Tunnel Mode)
SGW : N/A

Initialization:

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

```
    TGT_HOST2 ---------------------- TGT_HOST1
  HOST2_SA-O ----------------------> HOST1_SA-I
  HOST2_SA-I <---------------------- HOST1_SA-O
```

Security Association Database (SAD) for HOST1_SA-I

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

Security Policy Database (SPD) for HOST1_SA-I

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

Security Association Database (SAD) for HOST1_SA-O

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

Security Policy Database (SPD) for HOST1_SA-O

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

Security Association Database (SAD) for HOST2_SA-I

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

Security Policy Database (SPD) for HOST2_SA-I

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

Security Association Database (SAD) for HOST2_SA-O

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

Security Policy Database (SPD) for HOST2_SA-O

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

Packets:

ICMP Echo Request within ESP tunnel

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

ICMP Echo Reply within ESP tunnel

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

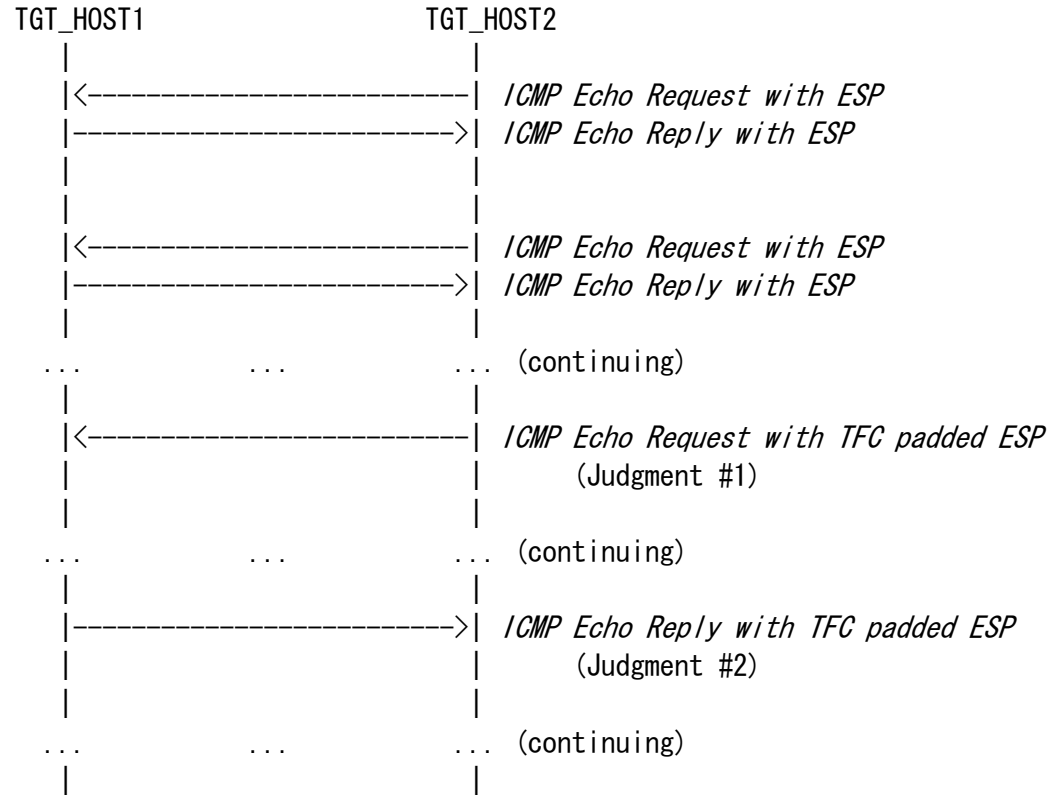
ICMP Echo Request within TFC padded ESP tunnel

IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ESP	SPI	0x1000
	Algorithm	3DES-CBC
	Key	ipv6readylogo3descbc2to1
	Authentication Algorithm	HMAC-SHA1
	Authentication Key	ipv6readylogsha12to1
	TFC padding	any size other than 0 byte
IP Header	Source Address	TGT_HOST2_Link1
	Destination Address	TGT_HOST1_Link0
ICMP	Type	128 (Echo Request)

ICMP Echo Reply within TFC padded ESP tunnel

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

Procedure:



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

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

Judgment:

Judgment #1
  Step-2: TGT_HOST2 transmits *"ICMP Echo Request with TFC padded ESP"*
Judgment #2
  Step-3: TGT_HOST1 transmits *"ICMP Echo Reply with TFC padded ESP"*

References:

RFC 4303: IP Encapsulating Security Payload (ESP)

Appendix-A Required Data

When you apply for an IPv6 Ready Logo Phase-2(IPsec) you need to submit test logs. In this appendix the detail requirement for the test log is described.

1.1. Required Data Type

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

A) Topology map

Network topology figures or address list, with IPv6 addresses and MAC address of each attached interfaces, are required. Fig.4 is an example of topology figure.

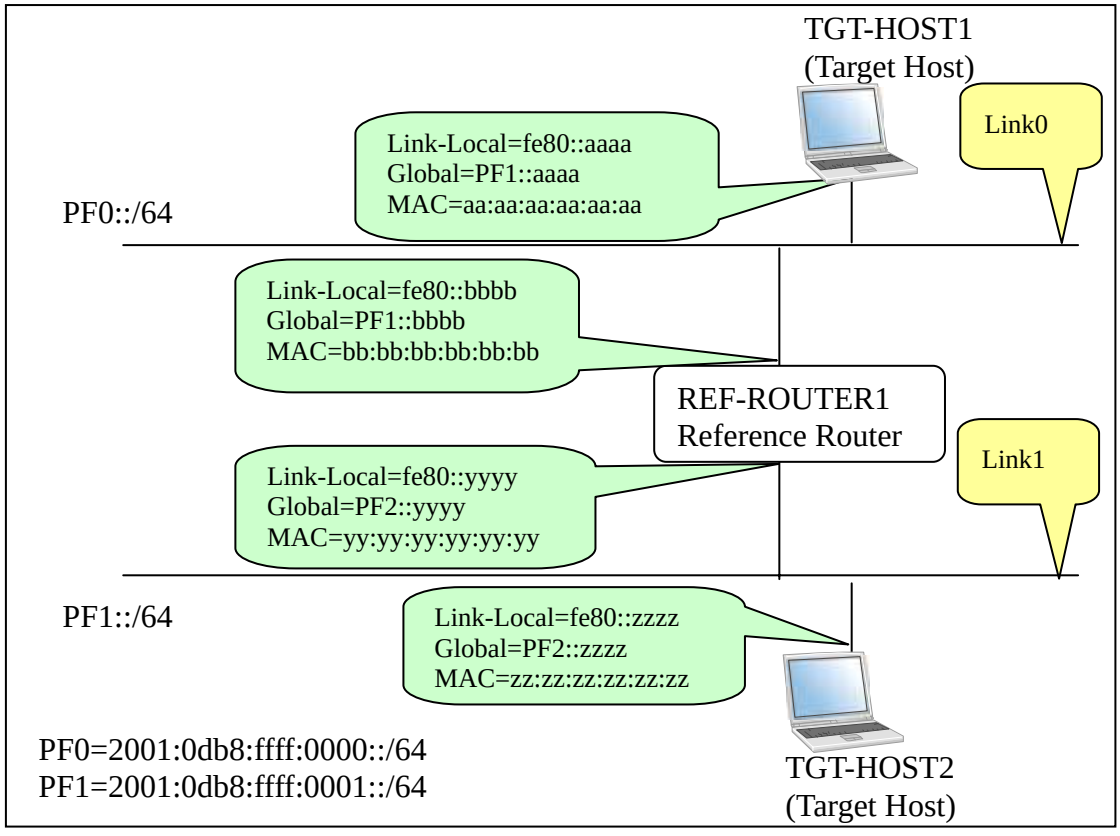


Fig. 4 Topology map example

Fig.5 is an example of address list.

TGT_HOST1:
Link-Local=fe80::aaaa
Global=PF1::aaaa
MAC=aa:aa:aa:aa:aa:aa

REF_ROUTER1 [Link0]:
Link-Local=fe80::bbbb
Global=PF1::bbbb
MAC=bb:bb:bb:bb:bb:bb

REF_ROUTER1 [Link1]:
Link-Local=fe80::yyyy
Global=PF2::yyyy
MAC=yy:yy:yy:yy:yy:yy

TGT_HOST2:
Link-Local=fe80::zzzz
Global=PF2::zzzz
MAC=zz:zz:zz:zz:zz:zz

Fig. 5 Address List example

B) Command Log

Ping is used as default application. When you run test with ping application, please save the command log into individual files.
We allow using other protocol than ICMP Echo Request and Reply. Even though you use other kind of application, please save the command log.
Save the command files for each test on each node.

C) Packet Capture File

Capture all packets on each link during the test with a device that is not part of the test.
Make individual tcpdump(pcap) format file for each test and link or put

the packet dump in a readable HTML file.

If you run tcpdump, please specify packet size as 4096.

e.g.,) tcpdump -i if0 -s 4096 -w 5.1.A.VendorA.Link0.dump

D) Test Result Table

Collect all test result tables in a file and fill the tables as required.

This file must contain a table where all passes are clearly marked.

1.2. Data file name syntax

Please use following syntax in the file name.

A) Topology Map

Chapter.Section.ON.topology

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

e.g.,)

If your device is a kind of End-Node, the name should be like following.

ON: Host [vendor: VendorA, model: rHost1, version: 1.0]

5.1. VendorA.topology.

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

ON: Router [vendor: VendorB, model: rRouter1, version: 2.0]

5.2.VendorB.topology

B) Command Results

Chapter.Section.Sub_Section.SRC.DST.result

For "*SRC*", use the vendor name on which the commands were run. If SRC is a Reference Host, just specify REF-Host*n* as SRC. For "*DST*", use the vendor name to which the commands were run, in other word, destination of ping command. If SRC is a Reference Host, just specify REF-Host*n* as DST

e.g.,)

Typical Naming sample are following.

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

TGT-Host1: Host [vendor: VendorA, model: rHost1, version: 1.0]

TGT-Host2: Host [vendor: VendorB, model: rHost2, version: 2.0]

5.1.1.VendorB.VendorA.result

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

TGT-Router1: Host [vendor: VendorA, model: rHost1, version: 1.0]

TGT-Router2: Host [vendor: VendorB, model: rHost2, version: 2.0]

REF-Host1: Host [vendor: VendorC, model: rHost1, version: 1.0]

REF-Host2: Host [vendor: VendorD, model: rHost2, version: 2.0]

5.2.1.REF-Host2.REF-Host1.result

C) Captured packet file

Syntax:*Chapter.Section.Sub_Section.ON.Link.dump*

For *"Link"*, use the captured link name.

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

Even if the command run on a Reference Node, you should list ON's vendor name rather than REF-Host*n*.

e.g.,)

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

TGT-Host1(Your Device):

Host [vendor: VendorA, model: rHost1, version: 1.0]

TGT-Host2(Opposite side device):

Host [vendor: VendorB, model: rHost2, version: 2.0]

5.1.A.VendorB.Link0.dump

5.1.A.VendorB.Link1.dump

D) Test Result Table

Syntax: *Vendor.table*

In this file you must make table for each sub-section.

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

	VendorA(HOST)	VendorB(HOST)
Applicants_name(HOST)		

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

	VendorC(ROUTER)	VendorD(ROUTER)
Applicants_name(HOST)		

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

	VendorA(HOST)	VendorB(HOST)
Applicants_name(ROUTER)		

For SGW vs. SGW tests, following table is required.

	VendorC(ROUTER)	VendorD(ROUTER)
Applicants_name(ROUTER)		

e.g.,)

Test result of following host.

TAR-Host1: Host [vendor: VendorA, model: rHost1, version: 1.0]

VendorA.table

1.3. Data Archive

Please organize your data as following directory structure.

```
$YourDeviceName_ver/
      Conformance/
      Interoperability/
```

Put all interoperability data file in "Interoperability" directory.

Put all conformance Self-Test results or conformance Lab test results in "Conformance" directory.

Make a tar.gz format archive file, and put all files under "$YourDeviceName_ver" in it.

****