

Moonv6 Test Suite
*IPSec Interoperability
Test Suite*

Technical Document

Version 1.0



*IPv6 Consortium
InterOperability Laboratory
Research Computing Center
University of New Hampshire*

*121 Technology Drive, Suite 2
Durham, NH 03824
Phone: (603) 862-2804
Fax: (603) 862-4181
<http://www.iol.unh.edu>*

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
MODIFICATION RECORD.....	ii
ACKNOWLEDGEMENTS.....	iii
INTRODUCTION.....	iv
COMMON TOPOLOGIES.....	iv
REFERENCES.....	vi
GROUP 1: Transport Mode.....	1
Test IPsec_INTEROP.1.1: Transport ESP_3DES_CBC HMAC_SHA1.....	2
Test IPsec_INTEROP.1.2: Transport ESP_3DES_CBC AES-XCBC.....	4
Test IPsec_INTEROP.1.3: Transport ESP_3DES_CBC NULL.....	6
Test IPsec_INTEROP.1.4: Transport ESP_3DES_CBC HMAC_MD5.....	8
Test IPsec_INTEROP.1.5: Transport ESP_AES_CBC HMAC-SHA1 (128-bit).....	10
Test IPsec_INTEROP.1.6: Transport ESP_NULL.....	12
Test IPsec_INTEROP.1.7: Transport ESP_DES_CBC.....	14
Test IPsec_INTEROP.1.8: Transport Mode Fragmentation.....	16
GROUP 2: Tunnel Mode.....	18
Test IPsec_INTEROP.2.1: Tunnel ESP_3DES_CBC HMAC_SHA1.....	19
Test IPsec_INTEROP.2.2: Tunnel ESP_3DES_CBC AES-XCBC.....	21
Test IPsec_INTEROP.2.3: Tunnel ESP_3DES_CBC NULL.....	23
Test IPsec_INTEROP.2.4: Tunnel ESP_3DES_CBC HMAC_MD5.....	25
Test IPsec_INTEROP.2.5: Tunnel ESP_AES_CBC HMAC-SHA1 (128-bit).....	27
Test IPsec_INTEROP.2.6: Tunnel ESP_NULL.....	29
Test IPsec_INTEROP.2.7: Tunnel ESP_DES_CBC.....	31
Test IPsec_INTEROP.2.8: Tunnel Mode Path MTU discovery and Fragmentation.....	33

MODIFICATION RECORD

Version 0.1	September 13, 2003 Initial Version
Version 1.0	November 15, 2005 Moonv6 Updates

ACKNOWLEDGEMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite:

Timothy Carlin	University of New Hampshire
Benjamin Schultz	University of New Hampshire
Timothy Winters	University of New Hampshire

INTRODUCTION

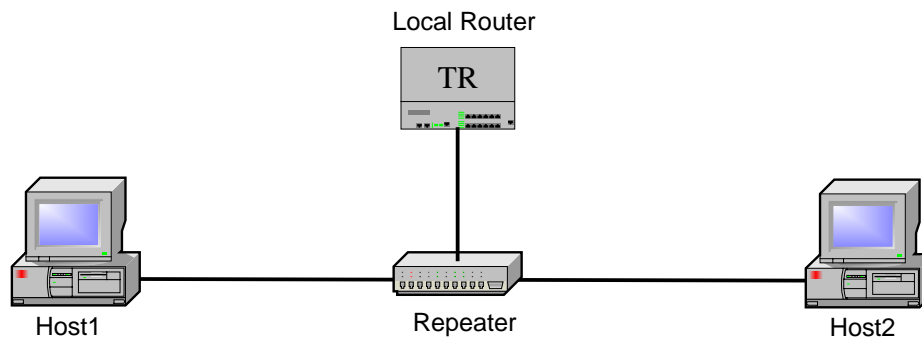
Overview

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard. This suite of tests has been developed to help implementers evaluate the functionality of their IPsec based products. This test suite has been designed to test interoperability of the device under test with other IPsec capable devices. This test suite focuses on testing configurations of the network that could cause problems when deployed if the device under test does not operate properly with the devices that it is connected to.

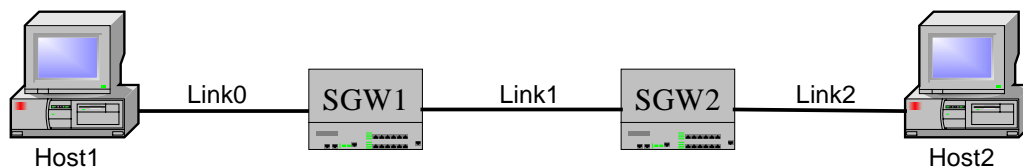
The tests do not determine if a product conforms to the IPsec standard but they are designed as interoperability tests. These tests provide one method to isolate problems within the IPsec capable device that will affect the interoperability performance. Successful completion of all tests contained in this suite does not guarantee that the tested device will operate with other IPsec capable devices. However, these tests do provide a reasonable level of confidence that the RUT will function well in most IPsec environment.

COMMON TOPOLOGIES

Transport Mode



Tunnel Mode



*University of New Hampshire
InterOperability Laboratory*

TEST ORGANIZATION

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

- Test Label:** The test label and title comprise the first line of the test block. The test label is composed by concatenating the short test suite name, the group number, and the test number within the group, separated by periods. The **Test Number** is the group and test number, also separated by a period. So, test label IPsec_INTEROP.1.2 refers to the second test of the first test group in the IPsec InterOperability suite. The test number is 1.2.
- Purpose:** The Purpose is a short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the feature or capability to be tested.
- References:** The References section lists cross-references to the specifications and documentation that might be helpful in understanding and evaluating the test and results.
- Resource Requirements:** The Resource Requirements section specifies the software, hardware, and test equipment that will be needed to perform the test.
- Discussion:** The Discussion is a general discussion of the test and relevant section of the specification, including any assumptions made in the design or implementation of the test as well as known limitations.
- Test Setup:** The Test Setup section describes the configuration of all devices prior to the start of the test. Different parts of the procedure may involve configuration steps that deviate from what is given in the test setup. If a value is not provided for a protocol parameter, then the protocol's default is used for that parameter.
- Procedure:** This section of the test description contains the step-by-step instructions for carrying out the test. These steps include such things as enabling interfaces, unplugging devices from the network, or sending packet from a test station. The test procedure also cues the tester to make observations, which are interpreted in accordance with the observable results given for that test part.
- Observable Results:** This section lists observable results that can be examined by the tester to verify that the RUT or the HUT is operating properly. When multiple observable results are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail for each test is usually based on how the RUT's behavior compares to the results described in this section.
- Possible Problems:** This section contains a description of known issues with the test procedure, which may affect test results in certain situations.

REFERENCES

The following documents are referenced in this text:

- [IPSecArch] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998
- [AH] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, November 1998
- [ESP] S. Kent, R. Atkinson, IP Encapsulating Security Payload, RFC 2406, November 1998
- [HMAC-SHA1] C. Madson, R. Glenn, The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998
- [DES-CBC] P. Karn, P. Metzger, W. Simpson, The ESP DES-CBC Transform, RFC 1829, August 1995
- [3DEC-CBC] P. Karn, P. Metzger, W. Simpson, The ESP Triple DES Transform, RFC 1851, September 1995
- [HMAC-MD5-96] C. Madson, R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 2403, November 1995
- [DES-CBC Cipher] C. Madson, N. Doraswamy, The ESP DES-CBC Cipher Algorithm with Explicit IV, RFC 2405, November 1998
- [NULL] R. Glenn, S. Kent, The NULL Encryption Algorithm and Its Use With IPsec, RFC 2410, November 1998
- [ICMPv6] A. Conta, S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol 6 (IPv6) Specification, RFC 2463, December 1998
- [AES-CBC] S. Fankel, R. Glenn, S. Kelly, The AES-CBC Cipher Algorithm and Its Use with IPsec, RFC 3602, September 2003
- [AES-XCBC] S. Frankel, H. Herbert, The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec, RFC 3566, September 2003

GROUP 1: Transport Mode

Scope:

The following tests are designed to verify that the hosts can successfully communicate with each other when Encapsulating Security Payload transport mode is in use.

Test IPsec_INTEROP.1.1: Transport ESP_3DES_CBC HMAC_SHA1

Purpose: To verify transport mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

*University of New Hampshire
InterOperability Laboratory*

Procedure:

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.2: Transport ESP_3DES_CBC AES-XCBC

Purpose: To verify transport mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	moonv6iolunhaesxin01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	moonv6iolunhaesxout1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

*University of New Hampshire
InterOperability Laboratory*

Procedure:

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packet transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.3: Transport ESP_3DES_CBC NULL

Purpose: To verify transport mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

*University of New Hampshire
InterOperability Laboratory*

Procedure:

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packet transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.4: Transport ESP_3DES_CBC HMAC_MD5

Purpose: To verify transport mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-MD5
ESP authentication key	moonv6unhiolmd50

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-MD5
ESP authentication key	moonv6unhiolmd50

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.5: Transport ESP_AES_CBC HMAC-SHA1 (128-bit)

Purpose: To verify transport mode with AES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC
ESP key	moonv6unhaescin0
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	AES-CBC
ESP key	moonv6unhaescout
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.6: Transport ESP_NULL

Purpose: To verify transport mode with AES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.7: Transport ESP_DES_CBC

Purpose: To verify transport mode with DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	DES-CBC
ESP key	idesin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	DES-CBC
ESP key	idesout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply with ESP to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply with ESP to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.1.8: Transport Mode Fragmentation

Purpose: Verify that devices can handle fragmented IPv6 Packets in an IPsec protected network.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use and it becomes necessary due to Path MTU restrictions to fragment packets.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	HOST1
destination address	HOST2
SPI	0x1000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	HOST1
destination address	HOST2
upper spec	any
direction	in
protocol	ESP
mode	transport

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	transport
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	HOST2
destination address	HOST1
upper spec	any
direction	Out
protocol	ESP
mode	transport

*University of New Hampshire
InterOperability Laboratory*

Procedure:

1. Configure Host1 and Host2 to have an MTU of 1280 on link 0.
2. Host1 transmits a 1400 byte ICMP Echo Request with ESP to Host2.
3. Observe the packets transmitted on link 0.
4. Host2 transmits a 1400 byte ICMP Echo Request with ESP to Host1.
5. Observe the packets transmitted on link 0.

Observable Results:

- **Step 3:** Host1 must transmit a fragmented ICMP Echo Request with ESP to Host2. Host2 must reply with a fragmented ICMP Echo Reply with ESP to Host1.
- **Step 5:** Host2 must transmit a fragmented ICMP Echo Request with ESP to Host1. Host1 must reply with a fragmented ICMP Echo Reply with ESP to Host2.

Observable Results:

- Hosts may not support a function for explicitly setting a Path MTU. If this is the case, Path MTU information can be acquired from the Local Router via a Router Advertisement.

GROUP 2: Tunnel Mode

Scope:

The following tests are designed to verify that the hosts can successfully communicate with each other when Encapsulating Security Payload tunnel mode is in use.

Test IPsec_INTEROP.2.1: Tunnel ESP_3DES_CBC HMAC_SHA1

Purpose: To verify tunnel mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_Link1
destination address	SGW2_Link1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	SGW1_Link1
destination address	SGW2_Link1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	HOST2
destination address	HOST1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	SGW1_Link1
destination address	SGW2_Link1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.2: Tunnel ESP_3DES_CBC AES-XCBC

Purpose: To verify tunnel mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW1_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	moonv6iolunhaesxin01

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	AES-XCBC-MAC-96
ESP authentication key	moonv6iolunhaesxout1

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packet transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.3: Tunnel ESP_3DES_CBC NULL

Purpose: To verify Tunnel mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	NULL
ESP authentication key	

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK2
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packet transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.4: Tunnel ESP_3DES_CBC HMAC_MD5

Purpose: To verify Tunnel mode with 3DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-MD5
ESP authentication key	moonv6unhiolmd50

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-MD5
ESP authentication key	moonv6unhiolmd50

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.5: Tunnel ESP_AES_CBC HMAC-SHA1 (128-bit)

Purpose: To verify tunnel mode with AES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC
ESP key	moonv6unhaescin0
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	AES-CBC
ESP key	moonv6unhaescout
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.6: Tunnel ESP_NULL

Purpose: To verify tunnel mode with AES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	Any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	NULL
ESP key	
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request with ESP to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request with ESP to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.7: Tunnel ESP_DES_CBC

Purpose: To verify tunnel mode with DES_CBC encryption.

Discussion: This test verifies that the hosts can successfully communicate with each other when Encapsulating Security Payload is in use.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	DES-CBC
ESP key	idesin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	DES-CBC
ESP key	idesout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

*University of New Hampshire
InterOperability Laboratory*

1. Host1 transmits an ICMP Echo Request to Host2.
2. Observe the packets transmitted on link 0.
3. Host2 transmits an ICMP Echo Request to Host1.
4. Observe the packets transmitted on link 0.

Observable Results:

- **Step 2:** Host2 must transmit an ICMP Echo Reply to Host1.
- **Step 4:** Host1 must transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.

Test IPsec_INTEROP.2.8: Tunnel Mode Path MTU discovery and Fragmentation

Purpose: Verify that devices can participate in path MTU discovery and handle fragmentation in an IPsec protected network.

Discussion: This test verifies that the hosts can successfully process Packet Too Big messages, and correctly fragment IP packets as a result.

Test Setup: Connect the network according to the [Common Topology](#). The following information can be configured either statically or dynamically. Configure Host1 and Host2 SAD and SPD as follows:

Security Association Database (SAD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
SPI	0x1000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcin01
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1in01

Security Policy Database (SPD) for SA-I

source address	SGW1_LINK1
destination address	SGW2_LINK1
upper spec	any
direction	in
protocol	ESP
mode	tunnel

Security Association Database (SAD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
SPI	0x2000
mode	tunnel
protocol	ESP
ESP algorithm	3DES-CBC
ESP key	moonv6unh-iol3descbcout1
ESP authentication	HMAC-SHA1
ESP authentication key	moonv6iolunhsha1out1

Security Policy Database (SPD) for SA-O

source address	SGW2_LINK1
destination address	SGW1_LINK1
upper spec	any
direction	Out
protocol	ESP
mode	tunnel

Procedure:

Part A:

1. Configure SGW2 to have an MTU of 1280 on its interface to Link2.
2. Host1 transmits at least 3 1400 byte ICMP Echo Requests to Host2.
3. Observe the traffic transmitted on all links.

Part B:

4. Configure SGW1 to have an MTU of 1280 on its interface to Link0.
5. Host2 transmits at least 3 1400 byte ICMP Echo Requests to Host1.
6. Observe the traffic transmitted on all links.

Observable Results:

Part A:

- **Step 3:** SGW2 should transmit a Packet Too Big message to Host1. Host1 should reduce its Path MTU estimate, and fragment its ICMP Echo Request for Host2. Host2 must reassemble the Echo Request, and transmit an ICMP Echo Reply to Host1.

Part B:

- **Step 6:** SGW1 should transmit a Packet Too Big message to Host2. Host2 should reduce its Path MTU estimate, and fragment its ICMP Echo Request for Host1. Host1 must reassemble the Echo Request, and transmit an ICMP Echo Reply to Host2.

Possible Problems:

- None.