

USGv6 Test Selection Tables*

IKEv2

F17-Conformance: IKEv2-v1.1

Applicable Profile: NIST SP 500-267 A profile for IPv6 in the U.S. Government - Version 1.0, July 2008.

Configuration Option: IKEv2

Test Specification Id:

- [[IKEv2-Conformance](#)] IPv6 Ready Logo Phase-2 Conformance Test Specification IKEv2, Version 1.1.0, June 8, 2010, [editor: [IPv6 Ready Logo](#)].

Reference:

- [RFC 4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
- [RFC 4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.
- [RFC 4868] Kelly, S., S. Frankel., "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

Device Type Definitions:

- **ROUTER:** A device capable of forwarding packets.
- **HOST:** A device which is not a ROUTER.
- **End-Node:** Both HOSTs and ROUTERs can be End-Nodes.
- **SGW:** A SGW is a specialized ROUTER.
* NOTE: if the Device Under Test is a ROUTER and it supports Tunnel Mode, it should be tested as a SGW.

IKEv2 Test Check List				
Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.1.1: Sending IKE_SA_INIT request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.1.2: Sending IKE_AUTH request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.1.3: Use of CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.2.1: Retransmissions of IKE_SA_INIT requests	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.2.2: Stop of retransmission of IKE_SA_INIT requests	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.2.3: Retransmissions of IKE_AUTH requests	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.2.4: Stop of retransmission of IKE_AUTH requests	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.1: State Synchronization with ICMP messages	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.2: State Synchronization with IKE messages	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.3: Close connections when repeated attempts fail	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.5.1: Retrying IKE_SA_INIT request with a Notify payload of type COOKIE	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (A) (H): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.2 (A) (C): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.9: Response with inconsistent SA proposal for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.10: Response with inconsistent proposal for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.7.1: Narrowing the range of members of the set of traffic selectors	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.10.1: Sending CERT Payload	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.10.3: RSA Digital Signature	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.10.4: HEX string PSK	End-Node	

RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.11.1: Non zero RESERVED fields in IKE_SA_INIT response	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.11.2: Non zero RESERVED fields in IKE_AUTH response	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.11.3: Version bit is set	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.11.4: Unrecognized Notify Message Type of Error	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.11.5: Unrecognized Notify Message Type of Status	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.1.1: Sending IKE_AUTH request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.1.2: Use of CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.1.1: Sending IKE_SA_INIT response	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.1.2: Sending IKE_AUTH response	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.1.3: Use of CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.2.1: Receipt of retransmitted IKE_SA_INIT request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.2.2: Receipt of retransmitted IKE_AUTH request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.1: State Synchronization with ICMP messages	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.2: State Synchronization with IKE messages	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.4: Receiving Liveness check	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.5: Receiving Delete Payload for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.6: Receiving Delete Payload for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.4.1: Receipt of a higher minor version number	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (A) (H): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.2 (A) (C): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.3: Receiving Multiple Transforms for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.4: Receiving Multiple Proposals for IKE_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.5: Receiving Multiple Transforms for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.6: Receiving Multiple Proposals for CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.8: Sending INVALID_KEY_PAYLOAD in Initial Exchange	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.7.1: Narrowing Traffic Selectors	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.7.3: Narrowing Traffic Selectors from multiple Traffic Selector	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.10.1: Sending Certificate Payload	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.10.3: RSA Digital Signature	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.10.4: HEX string PSK	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.11.1: Non zero RESERVED fields in IKE_SA_INIT request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.11.2: Non zero RESERVED fields in IKE_AUTH request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.11.3: Version bit is set	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.11.4: Response bit is set	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.11.5: Unrecognized Notify Message Type	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.3.1.1: Sending INFORMATIONAL response	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.3.2.1: Receipt of retransmitted INFORMATIONAL request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.3.3.1: Non RESERVED fields in INFORMATIONAL request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.2.1.1.1: Sending IKE_AUTH request	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.2.1.1.2: Use of CHILD_SA	End-Node	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.1.1: Sending IKE_SA_INIT request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.1.2: Sending IKE_AUTH request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.1.3: Use of CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.2.1: Retransmissions of IKE_SA_INIT requests	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.2.2: Stop of retransmission of IKE_SA_INIT requests	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.2.3: Retransmissions of IKE_AUTH requests	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.2.4: Stop of retransmission of IKE_AUTH requests	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.1: State Synchronization with ICMP messages	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.2: State Synchronization with IKE messages	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.3: Close connections when repeated attempts fail	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.5.1: Retrying IKE_SA_INIT request with a Notify payload of type COOKIE	SGW	

RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (A) (H): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.2 (A) (C): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.9: Response with inconsistent SA proposal for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.10: Response with inconsistent proposal for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.7.1: Narrowing the range of members of the set of traffic selectors	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.10.1: Sending CERT Payload	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.10.3: RSA Digital Signature	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.10.4: HEX string PSK	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.11.1: Non zero RESERVED fields in IKE_SA_INIT response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.11.2: Non zero RESERVED fields in IKE_AUTH response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.11.3: Version bit is set	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.11.4: Unrecognized Notify Message Type of Error	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.11.5: Unrecognized Notify Message Type of Status	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.2.1.1.1: Sending IKE_AUTH request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.2.1.1.2: Use of CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.1.1: Sending IKE_SA_INIT response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.1.2: Sending IKE_AUTH response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.1.3: Use of CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.2.1: Receipt of retransmitted IKE_SA_INIT request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.2.2: Receipt of retransmitted IKE_AUTH request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.1: State Synchronization with ICMP messages	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.2: State Synchronization with IKE messages	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.4: Receiving Liveness check	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.5: Receiving Delete Payload for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.6: Receiving Delete Payload for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.4.1: Receipt of a higher minor version number	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (A) (H): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.2 (A) (C): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.3: Receiving Multiple Transforms for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.4: Receiving Multiple Proposals for IKE_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.5: Receiving Multiple Transforms for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.6: Receiving Multiple Proposals for CHILD_SA	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.8: Sending INVALID_KE_PAYLOAD in Initial Exchange	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.7.1: Narrowing Traffic Selectors	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.7.3: Narrowing Traffic Selectors	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.10.1: Sending Certificate Payload	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.10.3: RSA Digital Signature	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.10.4: HEX string PSK	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.11.1: Non zero RESERVED fields in IKE_SA_INIT request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.11.2: Non zero RESERVED fields in IKE_AUTH request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.11.3: Version bit is set	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.11.4: Response bit is set	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.11.5: Unrecognized Notify Message Type	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.3.1.1: Sending INFORMATIONAL response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.3.2.1: Receipt of retransmitted INFORMATIONAL request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.3.3.1: Non RESERVED fields in INFORMATIONAL request	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.1.1: Sending IKE_AUTH response	SGW	
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.1.2: Use of CHILD_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-XCBC-MAC-96 SHOULD+ Tests

Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (D): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.2 (D): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (D): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.2 (D): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (D): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.2 (D): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (D): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.2 (D): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-XCBC-PRF-128 SHOULD+ Tests

Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (C): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (C): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (C): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4307	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (C): Cryptographic Algorithm Negotiation for IKE_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

HMAC-SHA-256-128 SHOULD+ Tests

Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (G): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.2 (G): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (G): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.2 (G): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (G): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.2 (G): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (G): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.2 (G): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

HMAC-SHA-256 as a PRF SHOULD+ Tests

Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (F): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (F): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (F): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4868	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (F): Cryptographic Algorithm Negotiation for IKE_SA	SGW	

NOTE: The following tests are considered a **SHOULD** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-CTR SHOULD Tests

Reference	Test Specification Id	Test Number	Device Type	Passed
-----------	-----------------------	-------------	-------------	--------

NOTE: The following tests have been omitted from the USGv6 Test Program for the IKEv2 Requirements. These tests are considered SHOULDs as defined by the IETF.

Not Required

Reference	Test Specification Id	Test Number	Device Type
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.4: Close connections when receiving INITIAL_CONTACT	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.4: Close connections when receiving INITIAL_CONTACT	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.5: Sending Liveness check	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.6: Sending Delete Payload for IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.7: Sending Delete Payload for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.3.8: Sending Liveness check with unprotected messages	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.4.1: Unrecognized payload types and Critical bit is not set	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.4.2: Unrecognized payload types and Critical bit is set	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.5.2: Interaction of COOKIE and INVALID_KE_PAYLOAD	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.5.2: Interaction of COOKIE and INVALID_KE_PAYLOAD	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Responder	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Responder	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.1 (B): Cryptographic Algorithm Negotiation for IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.1 (B): Cryptographic Algorithm Negotiation for IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.1 (B): Cryptographic Algorithm Negotiation for IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.1 (B): Cryptographic Algorithm Negotiation for IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.2 (B): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.2 (B): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.2 (B): Cryptographic Algorithm Negotiation for CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.2 (B): Cryptographic Algorithm Negotiation for CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.2 (E) (F): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.3 (A) (B) (C) (D): Sending Multiple Transforms for IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.4: Sending Multiple Proposals for IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.5 (A) (B) (C): Sending Multiple Transforms for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.6: Sending Multiple Proposals for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.7: Receipt of INVALID_KE_PAYLOAD	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.7: Receipt of INVALID_KE_PAYLOAD	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.8: Receipt of NO_PROPOSAL_CHOSEN	End-Node

RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.8: Receipt of NO_PROPOSAL_CHOSEN	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.11: Receipt of INVALID_KE_PAYLOAD in Initial Exchange	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.11: Receipt of INVALID_KE_PAYLOAD in Initial Exchange	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.1.6.12: Creating an IKE_SA without a CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.8.1: INVALID_IKE_SPI	End-Node
RFC 4306/4307	IKEv2-Conformance	Test IKEv2.EN.I.1.1.8.2: INVALID_SELECTORS	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.1.10.2: Sending CERTREQ Payload	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.1.1: Sending CREATE_CHILD_SA request	End-Node
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.I.1.2.1.1: Sending CREATE_CHILD_SA request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.2.1: Retransmissions of CREATE_CHILD_SA requests	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.2.2: Stop of retransmission of CREATE_CHILD_SA requests	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.1: Close the replaced CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.2: Use of the new CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.3: Lifetime of CHILD_SA expires	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.4: Sending Multiple Transform	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.5: Sending Multiple Proposal	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.6: Rekeying Failure	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.7: Perfect Forward Secrecy	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.3.8: Use of the old CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.1: Close the replaced IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.2: Use of the new IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.3: Lifetime of IKE_SA expires	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.4: Sending Multiple Transform	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.5: Sending Multiple Proposal	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.6: Use of the old IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.4.7: Changing PRFs when rekeying the IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.5.1: Create new CHILD_SA by sending CREATE_CHILD_SA request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.5.2: Receipt of cryptographically valid message on the new SA	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.1: Simultaneous CHILD_SA Close	End-Node
RFC 4718	IKEv2-	Test IKEv2.EN.I.1.2.6.2: Simultaneous IKE_SA Close	End-Node

	Conformance		
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.3: Simultaneous CHILD_SA Rekeying	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.4: Simultaneous CHILD_SA Rekeying with retransmission	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.5: Simultaneous IKE_SA Rekeying	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.6: Simultaneous IKE_SA Rekeying with retransmission	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.7: Rekeying a CHILD_SA while Closing a CHILD_SA	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.8: Closing a New CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.9: Rekeying a New CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.10: Rekeying an IKE_SA with half-open CHILD_SAs	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.11: Rekeying a CHILD_SA while rekeying an IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.12: Rekeying an IKE_SA with half-closed CHILD_SAs	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.13: Closing a CHILD_SA while rekeying an IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.14: Closing an IKE_SA while rekeying an IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.6.15: Rekeying an IKE_SA while Closing an IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.2.7.1: Non zero RESERVED fields in CREATE_CHILD_SA response	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.3.1.1: Sending INFORMATIONAL Exchange	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.3.2.1: Retransmission of INFORMATIONAL request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.3.2.2: Stop of retransmission of INFORMATIONAL request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.3.3.1: Non zero RESERVED fields in INFORMATIONAL response	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.1.3.4.1: INVALID_SPI	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.2.1: Sending CFG_REQUEST	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.2.2: Receipt of CFG_REPLY	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.2.3: Non zero RESERVED fields in Configuration Payload	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.2.4: Receipt of IKE_AUTH response without CFG_REPLY	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.I.2.1.2.5: Receipt of unrecognized Configuration Attributes	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.3: Close connections when receiving INITIAL_CONTACT	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.3.3: Close connections when receiving INITIAL_CONTACT	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.4.2: Receipt of a higher major version number	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.4.3: Unrecognized payload types and critical bit is not set	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.4.4: Unrecognized payload types and critical bit is set	End-Node

RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.4.5: Invalid Order Payloads	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.1: Cookies	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.1: Cookies	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.2: Invalid Cookies	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.2: Invalid Cookies	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.4: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Initiator	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.5.4: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Initiator	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.2 (E) (F): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.7: Sending INVALID_KE_PAYLOAD	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.7: Sending INVALID_KE_PAYLOAD	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.1.6.9: Creating an IKE_SA without a CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.7.2: TS_UNACCEPTABLE	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.8.3: INVALID_SELECTORS	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.8.1: INVALID_IKE_SPI	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.8.2: INVALID_SYNTAX	End-Node
RFC 4307	IKEv2-Conformance	Test IKEv2.EN.R.1.1.8.3: INVALID_SELECTORS	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.1.10.2: Sending Certificate Request Payload	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.1.1: Receipt of CREATE_CHILD_SA request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.2.1: Receipt of retransmitted CREATE_CHILD_SA request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.3.1: Receiving Delete Payload for Multiple CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.4.1: Sending NO_PROPOSAL_CHOSEN	End-Node
RFC 4718	IKEv2-Conformance	Test IKEv2.EN.R.1.2.4.1: Sending NO_PROPOSAL_CHOSEN	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.5.1: Close the replaced CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.5.2: Use of the new CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.5.3: Receiving Multiple Transform	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.5.4: Receiving Multiple Proposal	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.5.5: Perfect Forward Secrecy	End-Node
RFC 4306	IKEv2-	Test IKEv2.EN.R.1.2.5.6: Use of the old CHILD_SA	End-Node

	Conformance		
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.1: Sending CREATE_CHILD_SA response	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.2: Receipt of cryptographically valid message on the old SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.3: Receipt of cryptographically valid message on the new SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.4: Close the replaced IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.5: Receiving Multiple Transform	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.6: Receiving Multiple Proposal	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.7: Changing PRFs when rekeying the IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.6.8: D-H transform NONE when rekeying the IKE_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.7.1: Receipt of cryptographically valid message on the new SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.8.1: AUTHENTICATION_FAILED	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.EN.R.1.2.9.1: Non zero RESERVED fields in CREATE_CHILD_SA request	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.4: Close connections when receiving INITIAL_CONTACT	SGW
RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.4: Close connections when receiving INITIAL_CONTACT	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.5: Sending Liveness check	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.6: Sending Delete Payload for IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.7: Sending Delete Payload for CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.3.8: Sending Liveness check with unprotected messages	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.4.1: Unrecognized payload types and critical bit is not set	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.4.2: Unrecognized payload types and critical bit is set	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.5.2: Interaction of COOKIE and INVALID_KE_PAYLOAD	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Responder	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.3: Sending Multiple Transforms for IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.4: Sending Multiple Proposals for IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.2 (E) (F): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.5: Sending Multiple Transforms for CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.6: Sending Multiple Proposals for CHILD_SA	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.7: Receipt of INVALID_KE_PAYLOAD	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.8: Receipt of NO_PROPOSAL_CHOSEN	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.11: Receipt of INVALID_KE_PAYLOAD in Initial Exchange	SGW

RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.6.12: Creating an IKE_SA without a CHILD_SA	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.8.1: INVALID_IKE_SPI	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.8.2: INVALID_SELECTORS	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.1.10.2: Sending CERTREQ Payload	SGW
RFC 4306/4307	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.1.1: Sending CREATE_CHILD_SA request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.2.1: Retransmissions of CREATE_CHILD_SA requests	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.2.2: Stop of retransmission of CREATE_CHILD_SA requests	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.1: Close the replaced CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.2: Use of the new CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.3: Lifetime of CHILD_SA expires	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.4: Sending Multiple Transform	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.5: Sending Multiple Proposal	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.6: Rekeying Failure	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.7: Perfect Forward Secrecy	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.3.8: Use of the old CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.1: Close the replaced IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.2: Use of the new IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.3: Lifetime of IKE_SA expires	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.4: Sending Multiple Transform	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.5: Sending Multiple Proposal	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.6: Use of the old IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.4.7: Changing PRFs when rekeying the IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.5.1: Create new CHILD_SA by sending CREATE_CHILD_SA request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.5.2: Receipt of cryptographically valid message on the new SA	SGW
RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.1: Simultaneous CHILD_SA Close	SGW
RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.2: Simultaneous IKE_SA Close	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.3: Simultaneous CHILD_SA Rekeying	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.4: Simultaneous CHILD_SA Rekeying with retransmission	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.5: Simultaneous IKE_SA Rekeying	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.6: Simultaneous IKE_SA Rekeying with retransmission	SGW

	Conformance		
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.7: Rekeying a CHILD_SA while Closing a CHILD_SA	SGW
RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.8: Closing a New CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.9: Rekeying a New CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.10: Rekeying an IKE_SA with half-open CHILD_SAs	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.11: Rekeying a CHILD_SA while rekeying an IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.12: Rekeying an IKE_SA with half-closed CHILD_SAs	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.13: Closing a CHILD_SA while rekeying an IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.14: Closing an IKE_SA while rekeying an IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.6.15: Rekeying an IKE_SA while Closing an IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.2.7.1: Non zero RESERVED fields in CREATE_CHILD_SA response	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.3.1.1: Sending INFORMATIONAL Exchange	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.3.2.1: Retransmission of INFORMATIONAL request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.3.2.2: Stop of retransmission of INFORMATIONAL request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.3.3.1: Non zero RESERVED fields in INFORMATIONAL response	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.I.1.3.4.1: INVALID_SPI	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.3.3: Close connections when receiving INITIAL_CONTACT	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.4.2: Receipt of a higher major version number	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.4.3: Unrecognized payload types and critical bit is not set	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.4.4: Unrecognized payload types and critical bit is set	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.4.5: Invalid Order Payloads	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.5.1: Cookies	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.5.2: Invalid Cookies	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.5.3: Interaction of COOKIE and INVALID_KE_PAYLOAD	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.5.4: Interaction of COOKIE and INVALID_KE_PAYLOAD with unoptimized Initiator	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.2 (E) (F): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.7: Sending INVALID_KE_PAYLOAD	SGW
RFC 4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.6.9: Creating an IKE_SA without a CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.7.2: TS_UNACCEPTABLE	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.8.1: INVALID_IKE_SPI	SGW

RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.8.2: INVALID_SYNTAX	SGW
RFC 4306/4307	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.8.3: INVALID_SELECTORS	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.1.10.2: Sending Certificate Request Payload	SGW
RFC 4306/4307	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.1.1: Receipt of CREATE_CHILD_SA request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.2.1: Receipt of CREATE_CHILD_SA requests	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.3.1: Receiving Delete Payload for Multiple CHILD_SA	SGW
RFC 4306/4718	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.4.1: Sending NO_PROPOSAL_CHOSEN	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.1: Close the replaced CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.2: Use of the new CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.3: Receiving Multiple Transform	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.4: Receiving Multiple Proposal	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.5: Perfect Forward Secrecy	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.5.6: Use of the old CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.1: Sending CREATE_CHILD_SA response	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.2: Receipt of cryptographically valid message on the old SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.3: Receipt of cryptographically valid message on the new SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.4: Close the replaced IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.5: Receiving Multiple Transform	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.6: Receiving Multiple Proposal	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.7: Changing RPFs when rekeying the IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.6.8: D-H transform NONE when rekeying the IKE_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.7.1: Receipt of cryptographically protected message on the new SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.8.1: AUTHENTICATION_FAILED	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.1.2.9.1: Non zero RESERVED fields in CREATE_CHILD_SA request	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.2.1: Receipt of CFG_REQUEST	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.2.2: Use of CHILD_SA	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.2.3: Non zero RESERVED fields in Configuration Payload	SGW
RFC 4306	IKEv2-Conformance	Test IKEv2.SGW.R.2.1.2.4: No Configuration payload	SGW

* The objective of this test selection sheet is to provide a reference for available test specifications that identifies tests applicable to the USGv6 IPv6

Profile.