

# USGv6 Test Selection Tables\*

## ESP

**F29-Conformance:** ESP-v1.1

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

**Configuration Option:** ESP

**Test Specification Id:**

- [[IPsec-Conformance](#)] IPv6 Ready Logo Phase-2 Test Specification IPsec, Version 1.10.0, May 31, 2010, [editor: [IPv6 Ready Logo](#)].

**Reference:**

- [RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.
- [RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.
- [RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.
- [RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.
- [RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.
- [RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.
- [RFC4312] A. Kato, S. Moriai, and M. Kanda, "The Camellia Cipher Algorithm and Its Use With IPsec", RFC 4312, December 2005.
- [RFC4835] V. Manral, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.
- [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.

ESP Test Check List				
Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4835/2451/2404	IPsec-Conformance	5.2.1 Transport Mode ESP=3DES-CBC HMAC-SHA1	End-Node	
RFC 4835/3602	IPsec-Conformance	5.2.4 Transport Mode ESP=AES-CBC HMAC-SHA1	End-Node	
RFC 4835/2410	IPsec-Conformance	5.2.6 Transport Mode ESP=NULL HMAC-SHA1	End-Node	
RFC 4835/3602/2404	IPsec-Conformance	6.2.1 Tunnel Mode ESP=3DES-CBC HMAC-SHA1	SGW	
RFC 4835/3602	IPsec-Conformance	6.2.4 Tunnel Mode ESP=AES-CBC HMAC-SHA1	SGW	
RFC 4835/2410	IPsec-Conformance	6.2.6 Tunnel Mode ESP=NULL HMAC-SHA1	SGW	

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

AES/XCBC/MAC-96 SHOULD+ Tests				
Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4835/3566	IPsec-Conformance	5.2.2 Transport Mode ESP=3DES-CBC AES-XCBC	End-Node	
RFC 4835/3566	IPsec-Conformance	6.2.2 Tunnel Mode ESP=3DES-CBC AES-XCBC	SGW	

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

<b>AES-CTR SHOULD Tests</b>				
<b>Reference</b>	<b>Test Specification Id</b>	<b>Test Number</b>	<b>Device Type</b>	<b>Passed</b>
RFC 4835/3686	IPsec-Conformance	5.2.5 Transport Mode ESP=AES-CTR HMAC-SHA1	End-Node	
RFC 4835/3686	IPsec-Conformance	6.2.5 Tunnel Mode ESP=AES-CTR HMAC-SHA1	SGW	

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

<b>HMAC-SHA-256 SHOULD+ Tests</b>				
<b>Reference</b>	<b>Test Specification Id</b>	<b>Test Number</b>	<b>Device Type</b>	<b>Passed</b>
RFC 4835/4868	IPsec-Conformance	5.2.8 Transport Mode ESP=3DES-CBC HMAC-SHA-256	End-Node	
RFC 4835/4868	IPsec-Conformance	6.2.8 Tunnel Mode ESP=3DES-CBC HMAC-SHA256	SGW	

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

<b>Not Required</b>				
<b>Reference</b>	<b>Test Specification Id</b>	<b>Test Number</b>	<b>Device Type</b>	
RFC 4835	IPsec-Conformance	5.2.3. Transport Mode ESP=3DES-CBC NULL	End-Node	
RFC 4835	IPsec-Conformance	6.2.3. Tunnel Mode ESP=3DES-CBC NULL	SGW	
RFC 4835/4312	IPsec-Conformance	5.2.7 Transport Mode ESP=CAMELLIA-CBC HMAC-SHA1	End-Node	
RFC 4835/4312	IPsec-Conformance	6.2.7 Tunnel Mode ESP=CAMELLIA-CBC HMAC-SHA1	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.