USGv6 Test Selection Tables

IPv6 IPsec Requirements (IPsec, IKEv2)

**F11-Conformance:** Security Requirements R1v1.1

**Applicable Profile:** NIST SP 500-267B Revision 1 USGv6 Profile – November 2020.

**Test Specification Id:**


<table>
<thead>
<tr>
<th>Reference</th>
<th>Test Specification Id</th>
<th>Test Number</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>[RFC 8247]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation (A) AES128/SHA256/DH14 (B) AES256</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.1.4: IKE_SA_INIT Exchange with N(COOKIE)</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.1.7: IKE_SA_INIT inconsistent response proposal</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.1.8: IKE_SA_INIT Forward Compatibility (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.4: State Synchronization (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 8221]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.5: IKE_AUTH Cryptographic Algorithm Negotiation (A) AES128/SHA256 (B) AES256/SHA256 (D) AESGCM (F) NULL</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.6: IKE_AUTH N(NO_PROPOSAL_CHOSEN)</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.7: IKE_AUTH Inconsistent response proposal</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.8: Traffic Selector Negotiation</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.2.10: Authentication via RSA Digital Signature</td>
<td>SGW</td>
</tr>
<tr>
<td>[RFC 7296]</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.3.1: IKE_AUTH Request Format in Tunnel Mode</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.3.2: IKE_AUTH Exchange Succeeds in Tunnel Mode</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.5.1: IKE_SA Deletion</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.1.5.2: CHILD_SA Deletion</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.1: IKE_SA_INIT Response Format</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.2: IKE_SA_INIT Retransmission</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 8247</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation (A) AES128/SHA256/DH14 (B) AES256</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.4: IKE_SA_INIT Version Number (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.5: IKE_SA_INIT Multiple Transforms (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.6: IKE_SA_INIT Multiple Proposals</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.7: IKE_SA_INIT Exchange with INVALID_KE_PAYLOAD</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.8: IKE_SA_INIT Forward Compatibility (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.1.9: IKE_SA_INIT Invalid</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.3: IKE_AUTH Retransmission</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.4: State Synchronization (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 8221</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.5: IKE_AUTH Cryptographic Algorithm Negotiation (A) AES128/SHA256 (B) AES256/SHA256 (D) AESGCM (F) NULL</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.6: IKE_AUTH Multiple Transforms (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.7: IKE_AUTH Multiple Proposals</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.8: IKE_AUTH N(NO_PROPOSAL_CHOSEN)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.9: Traffic Selector Negotiation (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.10: Peer Identification (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.11: Authentication via RSA Digital Signature</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.12: Authentication via PSK (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.13: IKE_AUTH Forward Compatibility</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.2.14: Unrecognized Notify Type (A)(B)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.3.1: IKE_AUTH Response Format in Tunnel Mode</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.3.2: IKE_AUTH Exchange Succeeds in Tunnel Mode</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.5.1: INFORMATIONAL Exchange (A)(B)(C)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.5.2: IKE_SA Deletion</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 7296</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.1.2.5.3: CHILD_SA Deletion</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC 4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.1. Select SPD (2 SGW Peers)</td>
<td>SGW</td>
</tr>
<tr>
<td>RFC</td>
<td>Conformance</td>
<td>Test Case</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.2.</td>
<td>Select SPD (2 Hosts behind same Peer)</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.3.</td>
<td>Sequence Number Increment</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.4.</td>
<td>Packet Too Big Transmission</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.5.</td>
<td>Packet Too Big Forwarding</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.6.</td>
<td>Receipt of No Next Header (A)</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.7.</td>
<td>Bypass Policy</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.8.</td>
<td>Discard Policy</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.9.</td>
<td>Tunnel Mode Padding (A)(B)</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.10.</td>
<td>Invalid SPI</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.11.</td>
<td>Invalid ICV</td>
</tr>
<tr>
<td>4301</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.3.1.12.</td>
<td>Tunnel Mode with End-Node</td>
</tr>
<tr>
<td>8221</td>
<td>IPsec-Conformance</td>
<td>IPsec.Conf.4.1.3.</td>
<td>SGW ESP Algorithms</td>
</tr>
</tbody>
</table>

(A) AES128 / SHA256
(B) AES256 / SHA256
(D) NULL / SHA256
(G) AESGCM128 / N/A
(H) AESGCM256 / N/A
(I) AESGMAC128 / N/A
(J) AESGMAC256 / N/A
The objective of this test selection sheet is to provide a reference for available test specifications that identifies tests applicable to the USGv6 Profile.