# 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:**

- [IPsec Conformance] IPv6 Ready Test Specification IPsec and IKEv2, [editor: IPv6 Ready Logo ].

| IPsec-VPN Capability | | | |
|---|---|---|---|
| **Reference** | **Test Specification Id** | **Test Number** | **Device Type** |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.1.1: IKE_SA_INIT Request Format | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.1.2: IKE_SA_INIT Retransmission (A)(B) | SGW |
| [RFC 8247] | IPsec-Conformance | IPsec.Conf.1.1.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation<br>(A) AES128/SHA256/DH14<br>(B) AES256 | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.1.4: IKE_SA_INIT Exchange with N(COOKIE) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.1.7: IKE_SA_INIT inconsistent response proposal | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.1.8: IKE_SA_INIT Forward Compatibility (A)(B) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.3: IKE_AUTH Retransmission (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.4: State Synchronization (A)(B) | SGW |
| [RFC 8221] | IPsec-Conformance | IPsec.Conf.1.1.2.5: IKE_AUTH Cryptographic Algorithm Negotiation<br>(A) AES128/SHA256<br>(B) AES256/SHA256<br>(D) AESGCM<br>(F) NULL | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.6: IKE_AUTH N(NO_PROPOSAL_CHOSEN) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.7: IKE_AUTH Inconsistent response proposal | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.8: Traffic Selector Negotiation | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.9: Peer Identification (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.10: Authentication via RSA Digital Signature | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.11: Authentication via PSK (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.12: IKE_AUTH Forward Compatibility | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.2.13: IKE_AUTH Unrecognized Error (A)(B) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.3.1: IKE_AUTH Request Format in Tunnel Mode | SGW |

| | | | |
|---|---|---|---|
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.3.2: IKE_AUTH Exchange Succeeds in Tunnel Mode | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.5.1: IKE_SA Deletion | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.1.5.2: CHILD_SA Deletion | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.1: IKE_SA_INIT Response Format | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.2: IKE_SA_INIT Retransmission | SGW |
| [RFC 8247] | IPsec-Conformance | IPsec.Conf.1.2.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation<br>(A) AES128/SHA256/DH14<br>(B) AES256 | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.4: IKE_SA_INIT Version Number (A)(B) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.5: IKE_SA_INIT Multiple Transforms (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.6: IKE_SA_INIT Multiple Proposals | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.7: IKE_SA_INIT Exchange with INVALID_KE_PAYLOAD | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.8: IKE_SA_INIT Forward Compatibility (A)(B) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.1.9: IKE_SA_INIT Invalid | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.3: IKE_AUTH Retransmission | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.4: State Synchronization (A)(B) | SGW |
| [RFC 8221] | IPsec-Conformance | IPsec.Conf.1.2.2.5: IKE_AUTH Cryptographic Algorithm Negotiation<br>(A) AES128/SHA256<br>(B) AES256/SHA256<br>(D) AESGCM<br>(F) NULL | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.6: IKE_AUTH Multiple Transforms (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.7: IKE_AUTH Multiple Proposals | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.8: IKE_AUTH N(NO_PROPOSAL_CHOSEN) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.9: Traffic Selector Negotiation (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.10: Peer Identification (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.11: Authentication via RSA Digital Signature | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.12: Authentication via PSK (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.13: IKE_AUTH Forward Compatibility | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.2.14: Unrecognized Notify Type (A)(B) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.3.1: IKE_AUTH Response Format in Tunnel Mode | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.3.2: IKE_AUTH Exchange Succeeds in Tunnel Mode | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.5.1: INFORMATIONAL Exchange (A)(B)(C) | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.5.2: IKE_SA Deletion | SGW |
| [RFC 7296] | IPsec-Conformance | IPsec.Conf.1.2.5.3: CHILD_SA Deletion | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.1. Select SPD (2 SGW Peers) | SGW |

| | | | |
|---|---|---|---|
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.2. Select SPD (2 Hosts behind same Peer) | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.3. Sequence Number Increment | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.4. Packet Too Big Transmission | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.5. Packet Too Big Forwarding | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.6. Receipt of No Next Header (A) | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.7. Bypass Policy | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.8. Discard Policy | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.9. Tunnel Mode Padding (A)(B) | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.10. Invalid SPI | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.11. Invalid ICV | SGW |
| [RFC 4301] | IPsec-Conformance | IPsec.Conf.3.1.12. Tunnel Mode with End-Node | SGW |
| [RFC 8221] | IPsec-Conformance | IPsec.Conf.4.1.3. SGW ESP Algorithms<br>(A) AES128 / SHA256<br>(B) AES256 / SHA256<br>(D) NULL / SHA256<br>(G) AESGCM128 / N/A<br>(H) AESGCM256 / N/A<br>(I) AESGMAC128 / N/A<br>(J) AESGMAC256 / N/A | SGW |

**References:**


- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014. Online at: https://tools.ietf.org/html/rfc7296
- [RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, https://www.rfc-editor.org/info/rfc8221 .
- [RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017. Online at: https://tools.ietf.org/html/rfc8247
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, https://www.rfc-editor.org/info/rfc4301.


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