USGv6 Test Selection Tables

IPv6 IPsec Requirements (IPsec, IKEv2)

I11-Interoperability: Security Requirements R1v1.1

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

Test Specification Id:

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

Interoperability Partner Requirements:

- Any implementation claiming compliance with the USGv6 profile MUST demonstrate evidence of interoperability with three or more independent implementations of IPv6.
- The three implementations must include at least one End-Node and at least one SGW.
- Target nodes must not change once testing has begun.

IPsecv3-Interoperability

If your Device Under Test (DUT) Type is **End-Node**:

- DUT = TAR-EN1 for all tests.
- TAR-EN2 = Independent Implementation Device B
- TAR-SGW1 = Independent Implementation Device C
- Third Interoperability Partner is satisfied by executing the test specification again using the following:
    - TAR-SGW2 = Independent Implementation Device D
      or
    - TAR-EN3 = Independent Implementation Device D

Test Case Names – Test IPsec.IO.3.1, IPsec.IO.3.2
Appended to the name of these test cases is the topology and configuration required for the test run.

- EN.EN.1 – Configuration End-Node vs. End-Node 1, Transport, using Topo.EN.EN.1
- EN.EN.2 – Configuration End-Node vs. End-Node 2, Tunnel, using Topo.EN.EN.1
- EN.SGW.1 – Configuration End-Node vs. SGW 1, Tunnel, using Topo.EN.SGW.1

IPsec Capability			
Reference	**Test Specification Id**	**Test Number**	**Device Type**
[RFC 7296]	IPsec-Interoperability	IPsec.IO.1.1.1: Initiator Authentication (A)(B)(D)(E)(G)(H)	End-Node
[RFC 7296]	IPsec-Interoperability	IPsec.IO.1.1.2: Responder Authentication (A)(B)(D)(E)(G)(H)	End-Node
[RFC 7296]	IPsec-Interoperability	IPsec.IO.1.2.1 SA: Algorithm Mismatch (NO_PROPOSAL_CHOSEN) (A)(B)(D)(E)	End-Node
[RFC 7296]	IPsec-Interoperability	IPsec.IO.1.2.2 SA: Algorithm Mismatch (NO_PROPOSAL_CHOSEN) (A)(B)(D)(E)	End-Node
[RFC 7296]	IPsec-Interoperability	IPsec.IO.1.3: DH Retry (INVALID_KE_PAYLOAD) (B)(D)	End-Node
[RFC 7296] [RFC 4301] [RFC 4303]	IPsec-Interoperability	IPsec.IO.2.1: Basic Connection (A)(B)(C)	End-Node
[RFC 7296] [RFC 4301] [RFC 4303]	IPsec-Interoperability	IPsec.IO.2.2: Traffic Selectors (A)(B)(C)(E)(F)	End-Node
[RFC 7296] [RFC 4301] [RFC 4303]	IPsec-Interoperability	IPsec.IO.2.3: Fragmentation (A)(B)(C)(D)(E)(F)(G)	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.EN.1.IKESA.1: IKE_SA_INIT Algorithms	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.EN.1.IKESA.2: IKE_SA_INIT Algorithms	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.EN.2.IKESA.1: IKE_SA_INIT Algorithms	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.EN.2.IKESA.2: IKE_SA_INIT Algorithms	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.SGW.1.IKESA.1: IKE_SA_INIT Algorithms	End-Node
[RFC 8247]	IPsec-Interoperability	IPsec.IO.3.1.EN.SGW.1.IKESA.2: IKE_SA_INIT Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.1: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.2: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.4: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.7: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.8: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.9: IKE_AUTH Algorithms	End-Node

[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.1.IPSECSA.10: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.1: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.2: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.4: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.7: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.8: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.9: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.EN.2.IPSECSA.10: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.1: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.2: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.4: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.7: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.8: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.9: IKE_AUTH Algorithms	End-Node
[RFC 8221]	IPsec-Interoperability	IPsec.IO.3.2.EN.SGW.1.IPSECSA.10: IKE_AUTH Algorithms	End-Node

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.