Fusion Embedded™ IKE

Fusion Internet Key Exchange is an Internet Protocol security (IPsec) standard protocol used to ensure security for VPN negotiation and remote host or network access. It provides an automatic means of negotiation and authentication for IPsec security associations. IKE is a hybrid protocol that uses the framework defined by the Internet Security Association and Key Management Protocol (ISAKMP) together with key exchange concepts from the Oakley Key Determination Protocol (RFC 2412) and SKEME (A versatile and Secure Key Exchange Mechanism for the Internet) to obtain authenticated keying material for use with ISAKMP SAs and IPsec SAs.

Internet Key Exchange

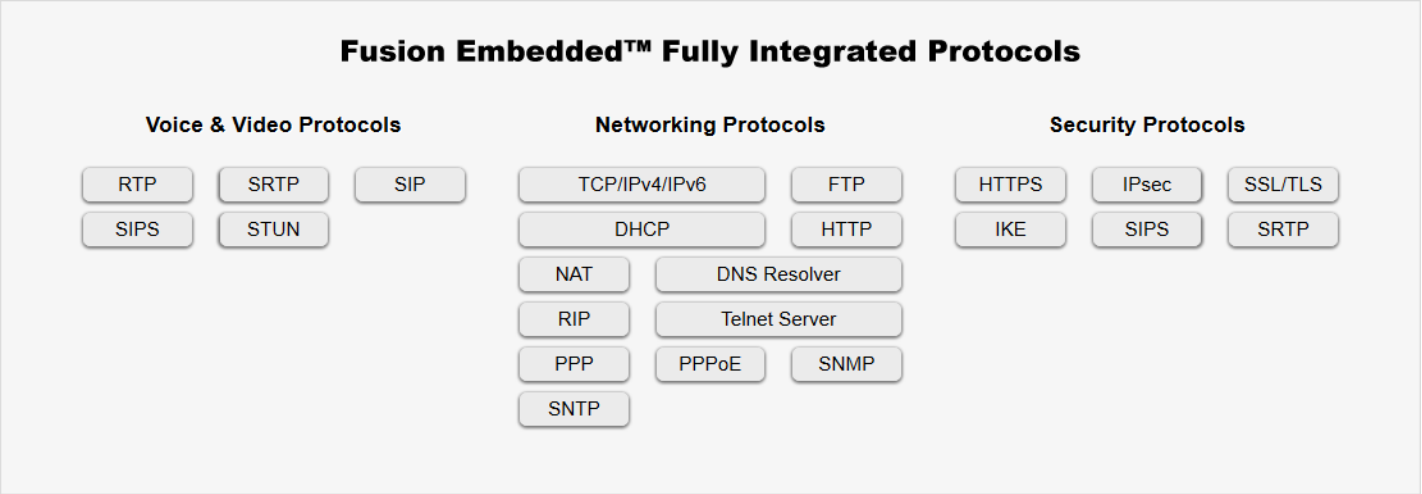
The Fusion implementation of the IKEv1 protocol is a high-performance, scalable, portable engine implementing the IKE protocol per RFCs 2407, 2408, and 2409. Fusion IKEv2 is an implementation of the IKEv2 Protocol as specified in RFC 4306.

Fusion Embedded IKEv2 Features

- Greater simplicity, and enhanced performance, security and reliability
- Support for Extensible Authentication Protocol (EAP)
- Legacy IKEv1 support, including support for ISAKMP (RFC 2408), IKE (RFC 2409), the Internet DOI (RFC 2407), NAT traversal, legacy authentication, and remote address acquisition.

Fusion Embedded IKEv2 Features

- Seamless integration with the Fusion IPsec kernel to provide a complete IP Security (IPsec) solution.
- High-performance, small foot-print
- Encryption with DES, 3DES, AES128 and Blowfish
- Authentication/Integrity with MD5 and SHA1
- Support for Perfect-Forward Secrecy
- Flexible run-time ISAKMP and IPsec policy configuration options including support for multiple proposal suites
- Main Mode IKE SA establishment
- Support for MODP (Oakley) groups 1 and 2
- Upgrade path to Version 2 of the IKE protocol



Email: info@unicoi.com **Phone**: +1 (678) 208-2250 All Rights Reserved. Copyright 2016. Unicoi Systems, Inc. 410 Peachtree Parkway, Cumming, GA 30041