Fusion Embedded™ IPsec

IP security (IPsec) provides cryptographically secured communication between applications that use the Internet Protocol. IPsec can be divided into two fundamental components–an IPsec "kernel", and an automated key exchange protocol such as the Internet Key Exchange (IKE).

The IPsec kernel runs below the socket layer and is responsible for the application of IPsec protection to individual IP datagrams. Key exchange protocols, such as IKE, which is the IETF standard key exchange protocol for IPsec, run above the sockets layer and enable communicating endpoints to automatically establish the keying material and other negotiable parameters (Security Associations) required for IPsec communications.

The Fusion Embedded IPsec kernel is a native IPsec implementation, as opposed to a Bump- in-the-stack (BITS, or "shim") implementation. It was written specifically for Fusion Embedded TCP/IPv4/IPv6, so it integrates cleanly with the Fusion Embedded TCP/IP stack.

Fusion Embedded IPsec provides a high-performance, minimal footprint solution that does not suffer from some of the problems with BITS implementations such as extra IP fragmentation and reassembly or partial duplication of IP stack functionality. The Fusion Embedded IPsec kernel uses no open source software and Fusion Embedded IKE is available separately.

IPsec Protocol Highlights

Strong encryption

Encrypting your system's Internet traffic means the content that is passed over the Internet cannot be easily read by intermediate nodes. The strength of the encryption refers to how easy it would be for the encrypted data to be 'cracked'. Fusion IPsec offers varying levels of encryption, and different encryption algorithms, trading off between processor usage and level of security.

Data integrity

By calculating a checksum and placing the checksum within the encrypted data, it can be made very difficult for the data that is passed over the Internet to be modified. Fusion IPsec automatically checks whether a packet received using IPsec has been tampered with. A modified packet is discarded and will normally be re-sent by the originator.

Peer Authentication

Authentication is achieved with digital signatures, meaning data recipients can be sure data received is from the real source. Replay Protection Duplicated packets (duplicated by an intermediate node on the Internet) can be prevented using an encrypted sequence number within the packet. Duplicate packets are discarded.

Other Product Notes

- Port available for MS Windows
- Both Transport and Tunnel modes are supported (Gateway and Host)
- Open configuration API
- Uses extensible PKI library written and designed for embedded systems with hooks for alternative cryptography providers including hardware assistance

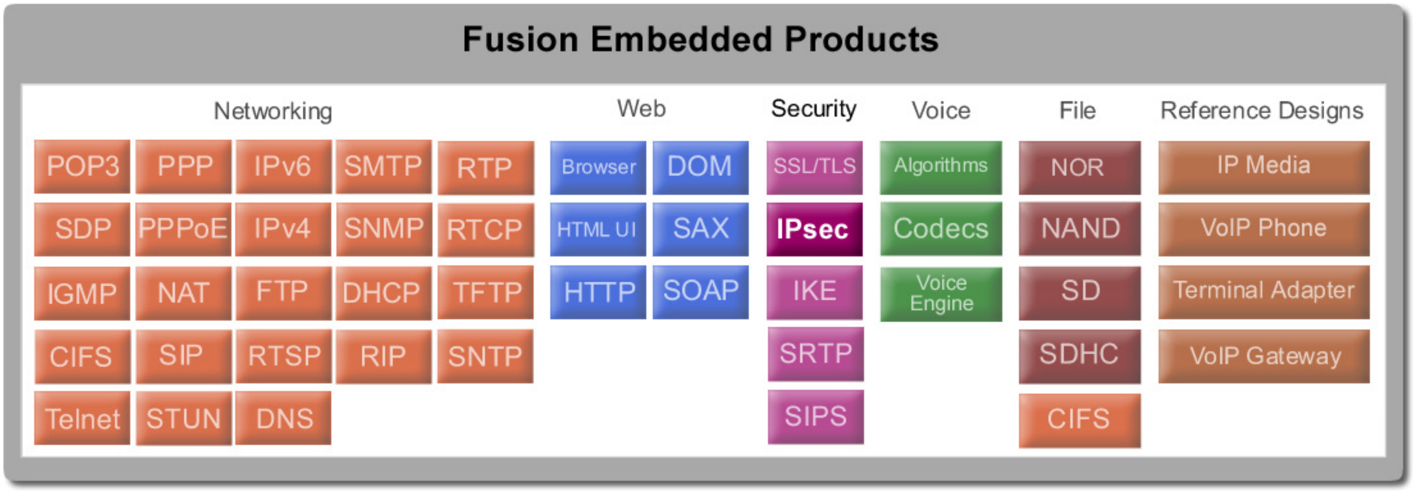
Features

- Native Fusion Net implementation – not a "Bump-in-the-Stack" shim
- Integrates with Fusion Intrnet Key Exchange (IKE) to provide a complete IPsec solution
- Support for ESP and AH in tunnel or transport mode, and ESP nested within AH (both in ransport mode)
- Powerful Security Policy Database semantics including the ability to configure bypass and drop policies, with application specified ordering of all SPD entries
- Global policies select whether the default for datagrams not matching any SPD entries is drop or bypass (default is drop)
- SPD selectors include source ad destination IPaddresses (address/prefix- length), upper layer protocol, source and destination ports for UDP and TCP including port ranges and wildcard, and also ICMP type and code including wild cards for either
- Support for the most popular encryption and MAC algorithms – DES, 3DES, AES3, and Blowfish for encryption, and MD5 or SHA1 for authentication
- Flexible configuration of ICMP error handling including options to ignore source address selector mismatches for ICMP error messages from routers
- Minimal additional copying of user data - for ESP authentication only (NULL encryption) and/or AH authentication no additional copies of user data required

- Utilizes Unicoi’s mPKI (micro Public Key I Infrastructure) library of cryptographic algorithms specifically developed for use in embedded systems. The mPKI library eliminates the need to port any opensource crypto libraries to your platform and provides high performance software cryptography and an abstraction layer that can be used to add hardware acceleration without modifications to the IPsec kernel code
- ‘Drop-in’ solution saving engineering cost and time-to-market
- Not based on Open Source: designed and written for embedded systems
- Manual Configuration of Security Associations (SA)
- Security policies based on individual or ranges of IP address(es), Port number(s) and/or protocol number
- Royalty-free license for OEMs
- ANSI C Embedded Source Code

IPsec RFC Compliance

- RFC 1321 (MD5 message digest)
- RFC 1829 (ESP DES-CBC Transform)
- RFC 1853 (IP in IP tunneling)
- RFC 2401 (Security Architecture for Internet Protocol)
- RFC 2402 (IP Authentication Header)
- RFC 2403 (The use of HMAC-MD5-96 within ESP and AH)
- RFC 2404 (The use of HMAC-SHA-1-96 within ESP and AH)
- RFC 2405 The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2406 (IP Encapsulation Security Payload)
- RFC 2410 (Null Encryption Algorithm and its use with IPsec)
- RFC 2451 (The ESP CBC-Mode Cipher Algorithm)
- RFC 3602 (The AES-CBC Cipher Algorithm and its use with IPsec)



Fusion Embedded Products

Networking					Web		Security	Voice	File	Reference Designs
POP3	PPP	IPv6	SMTP	RTP	Browser	DOM	SSL/TLS	Algorithms	NOR	IP Media
SDP	PPPoE	IPv4	SNMP	RTCP	HTML UI	SAX	IPsec	Codecs	NAND	VoIP Phone
IGMP	NAT	FTP	DHCP	TFTP	HTTP	SOAP	IKE	Voice Engine	SD	Terminal Adapter
CIFS	SIP	RTSP	RIP	SNTP			SRTP		SDHC	VoIP Gateway
Telnet	STUN	DNS					SIPS		CIFS	