



# V-IPSecure

## High-Velocity IP Layer Security

**V-IPSecure** is a high-performance, robust, lean and flexible implementation of IPsec and IKE for embedded operating systems. It provides IP extensions needed for security services at the network layer (Layer 3) along with advanced automatic key management. Unlike other protocols that secure individual network applications, IPsec protocols secure the connection at the network layer, thus automatically and transparently securing all network applications that use it. **V-IPSecure's** implementation of these protocols provides a high-quality cryptography-based communication channel that secures IP datagrams, when passing through intermediate nodes in a public network. This enables secure virtual private networks (VPN) to be carved out of a public and/or insecure networks. **V-IPSecure** is especially crafted for the stringent requirements of embedded systems focusing on small memory and flash footprints and high performance on embedded CPUs, including tight integration with specialized hardware. **V-IPSecure's** comprehensive and standards-compliant implementation makes it an ideal fit for embedded devices such as Internet appliances, VPN gateways, wireless devices, secure terminals, set-top boxes and routers.

### Secure Network Layer

Since security is not part of the original IP layer design, connected embedded devices need to implement security at

the application, transport, network, or link layer. Placing security at the network layer has several advantages, especially when security requirements affect all data going through the stack. Network layer security is transparent to the applications which use the network stack. Further, the security architecture is independent of the network type or topology to which the embedded device is connected and encrypted packets can be routed and switched on any network that supports IP traffic. **V-IPSecure** implements a secure network layer (IPsec) that provides data integrity, origin authentication, data confidentiality, access control, partial sequence integrity, and traffic flow confidentiality services for communications between any two networks or hosts. Replay-detection as defined by the IPsec standard is also performed by using sequence numbers combined with authentication.



Fig 1: Secure Network Layer

### The Security Advantage

**V-IPSecure** is a complete solution for network devices that require secure VPN or IPsec functionality. It also includes **Krypto-Lite**, TeamF1's FIPS-certified common crypto framework, along with a suite of encryption and integrity components to secure and manage access point traffic. **Krypto-Lite** also allows the seamless integration of other optional security protocols developed by TeamF1 such as SSL/https, SSH, Kerberos and others to meet additional security requirements.

### Features

- ❖ Support for the latest standards - AHv3, ESPv3, IKEv2, NAT-T
- ❖ IPComp payload compression
- ❖ Tunnel and Transport Mode
- ❖ Manual / Automated Key Exchange
- ❖ Includes TeamF1's Krypto-Lite crypto library with FIPS certified algorithms (3DES / AES / SHA)
- ❖ IKE authentication with pre-shared keys, RSA digital signatures, X.509 certificates and Kerberos
- ❖ IKE phase 1 Main & Aggressive Mode, Phase 2 Quick Mode
- ❖ Support for advanced cipher modes including AES-CCM-128 and Diffie-Hellman groups: 1, 2, 5, 14, advanced SHA2 Message Digest Algorithms - SHA2-256, SHA2-384, SHA2-512
- ❖ Support for IPv6
- ❖ Configuration via commands or configuration file
- ❖ PF\_KEY v2 key management API
- ❖ UDP Encapsulation for NAT Traversal
- ❖ Support for cached policies / SAs
- ❖ Support for PMTU, PMTU propagations and soft SA lifetimes
- ❖ Extended Sequence Number support
- ❖ Support for Perfect Forward Secrecy (PFS) and Replay Protection
- ❖ Support for complex bundle option, sysctl based management and MIBs
- ❖ Includes TeamF1's Advanced Hardware Acceleration Framework(XLR8™)
- ❖ Support for CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/XScale
- ❖ Extensive interoperability and compliance tested
- ❖ CableLabs PacketCable compliance
- ❖ Royalty-free full source distribution

**Support for Standards**

V-IPSecure includes a complete set of standards-based protocols for IPsec-enabling a standard TCP/IP (IPv4 or IPv6) network stack. V-IPSecure supports the IPsec Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols including their latest versions -- AHv3 and ESPv3. It also includes support for compression (IPComp). Support is included for manual and automated key management with MKM and IKE respectively. V-IPSecure supports both versions of the IKE protocol -- the legacy IKEv1 and the newly standardized and more advanced IKEv2.

**Tunnel and Transport Modes**

Depending on the mechanism of secure IP packet transmission, V-IPSecure supports two types of security associations (SAs), which define the IPsec protocol mode in use:

**Transport mode SA:** A security association between two hosts used to secure the traffic of higher layer protocols.

**Tunnel mode SA:** A security association modeled similar to an IP-in-IP tunnel by encapsulating IP packets into new

packets suitable for secure connections between security gateways. Based on the application requirements, V-IPSecure may be configured in either mode or a mix of the two modes for different connections.

**Security Policy Management**

The flexibility and power of V-IPSecure is enhanced by a highly configurable framework for policy and secure channel management. It allows for a flexible set of rules to decide when to apply the security policies and when to skip them, and provides different levels of security setup. For example, a secure communication channel to one network node may consist of a simple authentication scheme for traffic in both directions, while a highly secure authentication and encryption scheme may be setup for other hosts or entire networks. The management control for such flexibility is provided through a user friendly interface to the Security Policy Databases. Policies may be specified using IP addresses or FQDN.

**Automatic Key Negotiation**

V-IPSecure includes an implementation of Internet Key Exchange (IKE) which

- ❖ IPsec configuration via sysctl facility
- ❖ Configurable anti-replay window dimension
- ❖ Support for explicit specification of IKE exchange
- ❖ Configurable handling of packets not compliant with an security policy
- ❖ Key/policy management via PF\_KEY API
- ❖ Designed for hardware acceleration
- ❖ Available in full-source format
- ❖ Customization hooks and callouts
- ❖ Unwanted components can be scaled out

provides automatic key negotiation based on a Diffie-Hellman key exchange. The implementation allows for a frequent renewal of the crypto keys for higher security without increasing key-lengths which may slow down the encryption process. Phase 1 Main & Aggressive Mode and Phase 2 Quick Mode are supported in V-IPSecure's IKE. Authentication can be achieved using built-in mechanisms such as pre-shared keys or external mechanisms such as X.509 digital certificates, Kerberos GSSAPI and others. V-IPSecure's IKE is also completely interoperable with Microsoft Windows® implementations with pre-shared keys or using Active Directory as the authentication database. It also supports advanced cryptography including AES-CTR mode and AES XCBC-MAC.

**IKEv2 and NAT-T**

V-IPSecure also provides support for newer, more advanced Internet Key Exchange protocol version 2 (IKEv2) for negotiating keys, which can coexist with IKEv1. IKEv2 is designed to be simpler and more efficient than IKEv1 for the most commonly deployed scenarios and introduces support for Extensible Authentication Protocol (EAP), which allows peers to authenticate each other using EAP. V-IPSecure's IKEv2 is designed to be reliable using a lock-step request-response protocol. The IPsec protocol, as proposed in the original standard, cannot be used in environments that use network address translation (NAT and NATP). To address

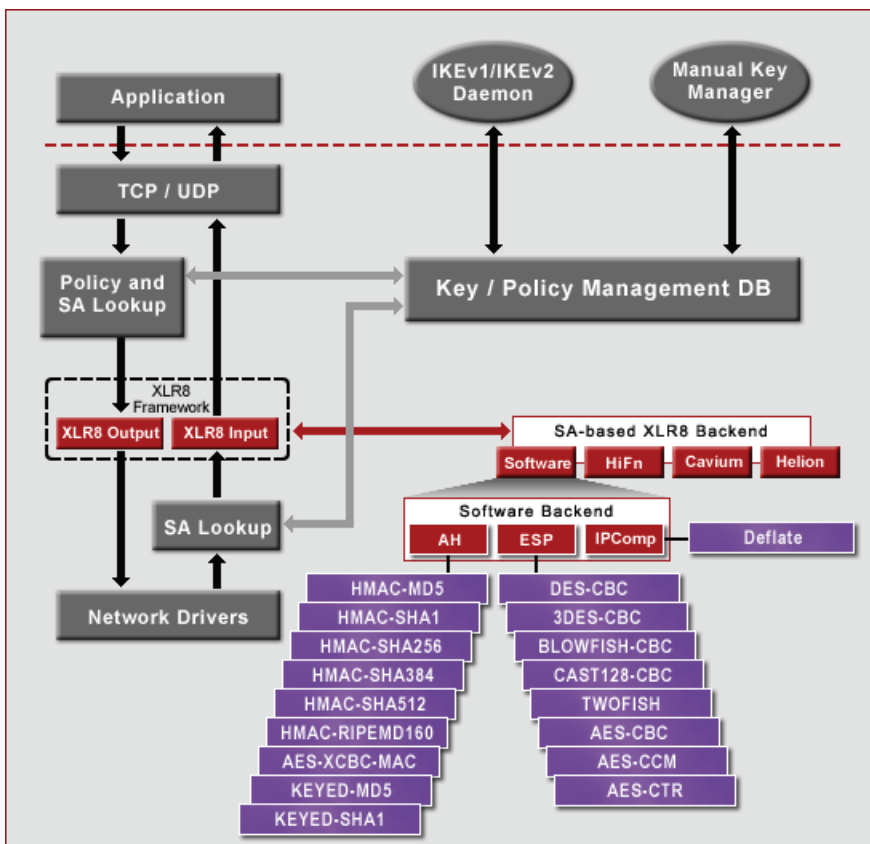


Fig 1: IPsec Architecture

the inherent incompatibilities between IPsec and NA(P)T, V-IPSecure provides support for the IETF standard for NAT-Traversal (NAT-T) of IPsec ESP applied on IPv4 packets.

### Hardware Acceleration

V-IPSecure has been designed and implemented to easily and efficiently allow for off-loading of IPsec functionality to Security Processors at a fine grain (algorithm) or coarse grain (protocol) level. Hardware acceleration not only increases maximum throughput, but also greatly reduces CPU load and power consumption. TeamF1's XLR8™ Hardware Acceleration Framework, is designed to allow various computationally intensive parts of networking software to be off-loaded to dedicated hardware, such as IPsec, checksum calculation, compression, Diffie-Hellman computation, etc. thereby enhancing the overall system efficiency and throughput. The XLR8 Framework provides a set of APIs that can be used to implement an XLR8 IPsec

implementation in software and/or hardware. Reference implementations are provided for IPsec Accelerators based on Hifn, Cavium and Xilinx (using Helion cores) chips.

### Advanced Features

V-IPSecure seamlessly integrates with any IPv4 or IPv6 based TCP/IP stack, leveraging features such as PMTU support if the native stack provides it. It also includes an implementation of PF\_KEY, a socket protocol family used by privileged key management applications to communicate with the kernel's key management databases, i.e. the Security Association database and the Security Policy database. V-IPSecure programmers can use this interface to write their own custom applications to conveniently interact with key databases. V-IPSecure also includes other advanced features such as bundled SAs, options to generate fine-grained/coarse grained SAs from same policy, support for cached policies and SAs, support for PMTU and soft SA

### Also Available

- ❖ **NetF1**  
*High Octane TCP/IP including IPV6*
- ❖ **S Secure Family**  
*Security protocols (SSL, SSH, IPsec/IKE)*
- ❖ **AuthAgents**  
*Authentication agents: Kerberos, RADIUS, X.509 Digital Certificates*
- ❖ **Switchcraft Suite**  
*802.n Switching components*

### Custom Solutions

TeamF1's professional services can provide the resources and expertise to build customized implementations of V-IPSecure including support for other authentication protocols, support for hardware accelerators, network processors off-load, and to provide scaled-down application-specific implementations.

lifetimes, Extended Sequence Number support, SA-based IP options, support for Perfect Forward Secrecy (PFS) and many others. V-IPSecure is also qualified with DNSSEC.

### OS and Hardware Support

V-IPSecure is designed to make efficient use of CPU processing power, memory, and OS resources given the stringent requirements of embedded systems. It has been extensively validated on a variety of CPU architectures, thus minimizing development and integration efforts. It makes use of the native network stack or can be configured to run in high-performance mode with TeamF1's NetF1 TCP/IP stack. V-IPSecure is available with optimized editions for VxWorks® and Linux® with support for the native network driver model, enhanced memory management.

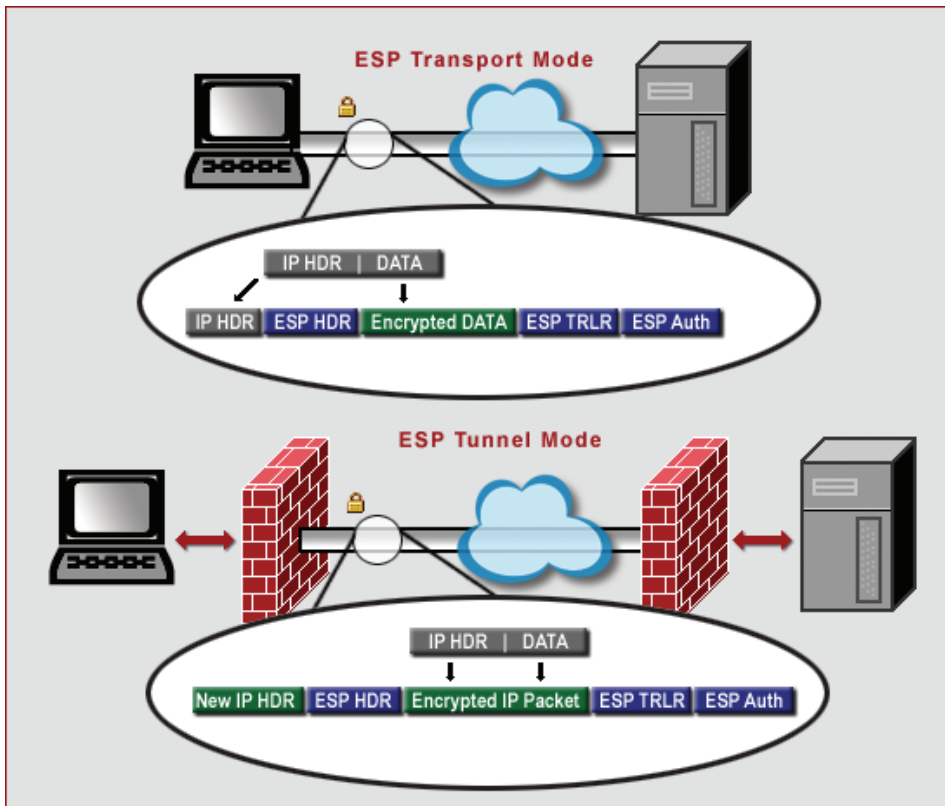


Fig 1: Transport & Tunnel Mode

## Supported RFCs

RFC	Status	Obsoletes	Description
<b>IPsec</b>			
1828	Proposed Standard		IP Authentication using Keyed MD5.
1829	Proposed Standard		The ESP DES-CBC Transform.
2085	Proposed Standard		HMAC-MD5 IP Authentication with Replay Prevention.
2104	Proposed Standard		HMAC: Keyed-Hashing for Message Authentication.
2394	Proposed Standard		IP Payload Compression Using DEFLATE.
2401	Proposed Standard	1825	Security Architecture for the Internet Protocol.
2402	Proposed Standard	1826	IP Authentication Header.
2403	Proposed Standard		The use of HMAC-MD5-96 within ESP and AH.
2404	Proposed Standard		The use of HMAC-SHA-1-96 within ESP and AH.
2405	Proposed Standard		The ESP DES-CBC Cipher Algorithm with Explicit IV.
2406	Proposed Standard	1827	IP Encapsulating Security Payload (ESP).
2410	Proposed Standard		The NULL Encryption Algorithm and its use with IPsec.
2411	Proposed Standard		IP Security Document Roadmap.
2451	Proposed Standard		The ESP CBC-Mode Cipher Algorithms.
3173	Proposed Standard	2393	IP Payload Compression Protocol (IPComp).
3554	Proposed Standard		On the use of Stream Control Transmission Protocol (SCTP) with IPsec
3602	Proposed Standard		The AES-CBC Cipher Algorithm and its use with IPsec
3686	Proposed Standard		Using AES Counter Mode with IPsec ESP
3948	Proposed Standard		UDP Encapsulation of IPsec Packets.
<b>Key Management</b>			
2367	Informational		PF_KEY Key Management API, Version 2.
2407	Proposed Standard		The Internet IP Security Domain of Interpretation for ISAKMP.
2408	Proposed Standard		Internet Security Association and Key Management Protocol (ISAKMP).
2409	Proposed Standard		The Internet Key Exchange (IKE).
2412	Proposed Standard		The OAKLEY Key Determination Protocol.
3526	Proposed Standard		More Modular Exponential Diffie-Hellman groups for Internet Key Exchange.
3947	Proposed Standard		Negotiation of NAT-Traversal in the IKE.

## Drafts Support

Draft	Description
draft-ietf-ipsec-esp-v3	IP Encapsulating Security Payload (ESP).
draft-ietf-ipsec-ikev2	Internet Key Exchange (IKEv2) Protocol.
draft-ietf-ipsec-rfc2402bis	IP Authentication Header.
draft-ietf-ipsec-esn-addendum	Extended Sequence Number Addendum to IPsec DOI for ISAKMP.
draft-ietf-ipsec-ciph-aes-ccm	Using AES CCM Mode with IPsec ESP.
draft-ietf-ipsec-ikev2-algorithms	Cryptographic Algorithms for use in the Internet Key Exchange Version 2.
draft-ietf-ipsec-rfc2401bis	Security Architecture for the Internet Protocol.
draft-ietf-ipsec-esp-ah-algorithms	Cryptographic Algorithm implementation requirements for ESP and AH.

Email: [sales@TeamF1.com](mailto:sales@TeamF1.com)  
 Web: [www.TeamF1.com](http://www.TeamF1.com)  
 Ph: 510-505-9931 ext. 5  
 Fax: (510) 505-9941



© 2011 TeamF1, Inc.