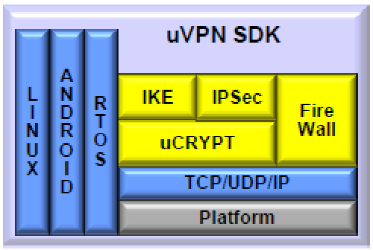
Cypherbridge® Systems

uVPN IKE/IPSec Software Development Kit

Overview

The Cypherbridge Systems uVPN SDK implements IKEv1/IKEv2/IPsec for a cryptographically secure solution for IP packet networking. It provides authentication, data encryption and message integrity for embedded devices. The uVPN SDK is a standards based, full featured toolkit delivering system benefits including security and performance for embedded platforms, smart phones, tablets and more. The uVPN SDK is optimized for deployment in embedded systems.

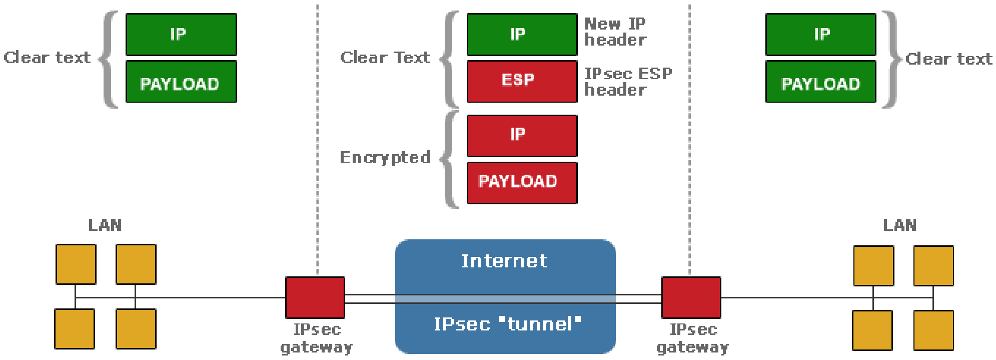
The uVPN SDK provides a unified solution combining IKE/IPsec network encryption, plus firewall defense, using a common set of policies that include IP address, port and protocol. These policies simultaneously firewall and block low level connections to the device, monitor traffic flows through the device, and encrypt and authenticate traffic with IKE/IPsec.



IPsec

IPsec adds peer authentication, encryption and message integrity to IP packet networks, protecting against loss of data privacy, integrity, identity spoofing, and replay attack. IPsec adds security at the network IP layer, with no changes needed to existing client/server or streaming applications. Widely adopted, standards based and interoperable with all network equipment, IPsec can be deployed in host-to-host security channels, road warrior VPN to corporate network, or network-to-network.

The uVPN SDK supports AH and ESP protocols, as illustrated in the following diagram showing ESP enscapulation over a network-to-network tunneled VPN:



Features

- ✓ *Supports IKEv2, IKEv1 responder, initiator, main and aggressive modes*
- ✓ *IPsec Tunnel, Transport, ESP and AH*
- ✓ *Streamlined IKEv2 initiator for smallest possible footprint*
- ✓ *Portable and compact ANSI-C library*
- ✓ *Administrator program and API toolkit for SPD/SAD policy configuration*
- ✓ *Flexible Firewall Configuration*
- ✓ *Android, RTOS, and Embedded Linux operating system support*
- ✓ *ARM, PowerPC, x86 processors*
- ✓ *Interoperates with Openswan, Strongswan, Windows Firewall and OpenBSD VPN*
- ✓ *Crypto Porting Layer and Suite B Option*

For Pricing and Availability Contact:

Cypherbridge Systems, LLC
7040 Avenida Encinas #104211
Carlsbad, CA 92011 USA
www.cypherbridge.com
sales@cypherbridge.com
Tel: +1 (760) 814-1575

About Cypherbridge Systems:

Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.

Product features and specifications subject to change without notice.

Features

- *Supports AH and ESP connections, tunnel, and transport mode*
- *Integrated uCrypt™ cryptographic library includes DHM, AES, 3DES, RC4, SHA1, MD5*
- *TCP/IP"bump-in-stack" interface integrates with RTOS, Kernel, and User Mode TCP/IP stacks*
- *Crypto Porting Layer and Suite B Option Available*

IKE- Internet Key Exchange

uVPN uIKE implements IKEv1 and IKEv2 standards based protocols to set up the Security Associations (SA) for IPsec. Peer systems dynamically establish and synchronize the IKE SA through mutual authentication and secure exchange of session keys.

The Security Policy Database (SPD) governs the policy and management of the security layers. The SPD is used to define traffic flows, such that selected network traffic and direction can be configured on a granular basis. This allows all or selected network traffic to be protected with IPsec.

uVPN uIKE stores the keys in the Security Association Database (SAD). IPsec fetches the cipher and authentication type and keys from the SAD, then applies security to an IP packet to encrypt outbound packets, and decrypt inbound packets.

Features

- *Supports embedded IKE initiator and responder roles, Phase1 and Phase2 Security Associations*
- *Configurable default and session options for IKE negotiation*
- *Automatic negotiation of IKE connection*
- *Authentication using shared secret and RSA key pairs*

Firewall

By combining IPsec and firewall features, the uVPN SDK has multiple levels of protection against cyber intrusion in a solution that reduces target memory footprint, time-to-market, and Total Cost of Ownership. Typically, users have had to integrate separate SDKs from multiple suppliers. Now, instead of having to configure and manage two different and complex system level SDKs, the uVPN unified SDK can be integrated on the target platform

Features

- *Firewall can be enforced at network L2 or IP layer L3*
- *Policies are unified with IPSec SPD Tables and Administration Application*
- *Flexible Policy Extensions for flow based packet inspection, counters and thresholds*

For Pricing and Availability Contact: Cypherbridge Systems, LLC 7040 Avenida Encinas #104211 Carlsbad, CA 92011 USA www.cypherbridge.com sales@cypherbridge.com Tel: +1 (760) 814-1575	***About Cypherbridge Systems:*** Established in 2005 to offer software, server, security, device and system level products, our portfolio includes software stacks to enable a broad range of connected device applications integrating embedded device, communications networks, and back office servers in a system solution.	Copyright © 2013 Cypherbridge Systems, LLC. Product features and specifications subject to change without notice. CSL-uVPN-0201.1