



Customised Algorithm Toolkit User Overview

Table of Contents

1. TOOLKIT OVERVIEW	3
1.1. Rock VPN overview	3
1.2. Architecture	4
2. DEFINITIONS AND ABBREVIATIONS	5
3. CONTACT DETAILS	5

1. TOOLKIT OVERVIEW

The Rock VPN Customised Algorithm Toolkit provides a mechanism for end users to add their own symmetrical cipher algorithms to Rock VPN. The toolkit is intended for users that are familiar with C programming on the platforms supported by the toolkit.

The Toolkit provides an API and software framework that allows users to build loadable software modules that can dynamically extend the cryptographic support of the Rock VPN products. Algorithms can be any combination of the supported block sizes of 64-bit, 128-bit and 256-bit.

Algorithms are pre-defined in the Rock VPN software, but unless they are replaced by user implementations using loadable modules, these algorithms will cause negotiations to fail when an IPSec session is attempted using any one of these algorithms.

Users may replace these algorithms by:

- Building modules to implement the user defined algorithms;
- Installing and loading these modules as per the documentation; and
- Changing the Rock VPN security policy to use these algorithms.

The user algorithms may have any key length that is a multiple of 8 bits, but must have a block length of 64 bits, 128 bits or 256 bits.

1.1. Rock VPN overview

The purpose of this section is not to give a complete overview of Rock VPN, but to highlight the components that will interact with the implemented algorithms.

The Rock VPN products implement the IPSec protocol suite, an IETF standard for securing traffic on the Internet. The IPSec protocol suite consists of traffic security protocols, cryptographic key management procedures and protocols that are used together to provide security at the network level. The IPSec protocol suite consists of the following:

- Authentication Header (AH) protocol
- Encapsulating Security Payload (ESP) protocol
- Internet Key Exchange (IKE), a combination of the Internet Security Association and Key Management Protocol and the Oakley key exchange (ISAKMP/Oakley)

The IKE protocol is the standard protocol for negotiating the security mechanisms to be used between two hosts. It securely produces random short-term session keys for the hosts, and authenticates the hosts using either shared secrets (passwords) or certificates.

ESP is used to provide confidentiality (encryption), data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

Proprietary symmetrical algorithms can be added to Rock VPN using the Customised Algorithm Toolkit. These algorithms can then be used by the ESP and IKE protocols to provide confidentiality.

1.2. Architecture

As discussed above, there are two components of Rock VPN that use symmetric algorithms, namely the IKE and ESP protocols. Figure 4.1 shows a block diagram of the components in Rock VPN and where the user supplied algorithms fit in.

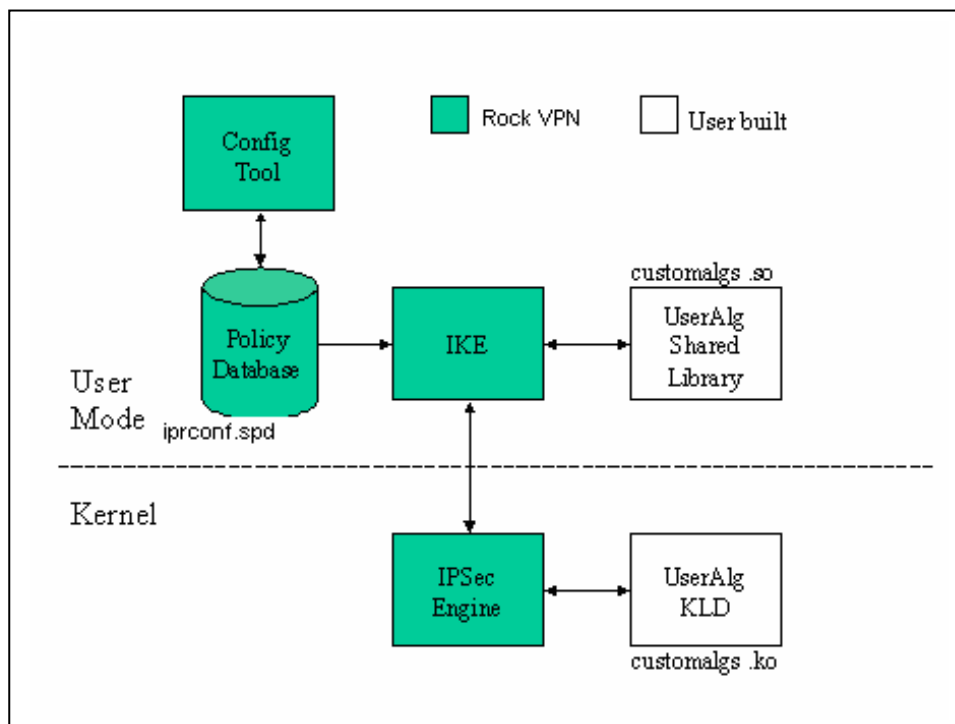


Figure 4.1: Block diagram showing the various components of Rock VPN on a FreeBSD system with custom user algorithms.

IKE is a user mode process, while the IPSec engine is linked into the kernel for optimised performance. This requires that two loadable modules be built to supply the custom algorithm(s). On the FreeBSD platform, IKE (IPSec policy manager) uses a shared library to access the custom algorithms, while ESP (in IPSec engine) uses a KLD (a loadable Kernel module) to access them.

The same algorithm implementation (source code) can be used to build the two loadable modules. Each loadable module must contain all the custom algorithms required as only one loadable module of each type (user and kernel) can be used.

2. DEFINITIONS AND ABBREVIATIONS

<i>AES</i>	Advanced Encryption Standard, the successor to DES. See Rijndael.
<i>Algorithm</i>	Used interchangeably with (block) cipher in this document.
<i>CBC</i>	Cipher Block Chaining, a feedback mode used on a block cipher.
<i>DES</i>	Data Encryption Standard, a 64-bit block cipher.
<i>ESP</i>	Encapsulating Security Payload (described in RFC 2406).
<i>FTP</i>	File Transfer Protocol.
<i>IKE</i>	Internet Key Exchange (described in RFC 2409).
<i>IV</i>	Initialisation Vector. This is an initialisation variable used in block cipher modes such as CBC.
<i>KLD</i>	A FreeBSD loadable kernel module.
<i>Rijndael</i>	The algorithm chosen for AES.

3. CONTACT DETAILS

Tel: +603-6203 5303
Fax: +603-6203 5302
URL: www.rockvpn.com

For more information or support requests, please visit www.rockvpn.com or www.mynetsec.com.