Configuring IPsec Profile Manual Keying Mode on RV160 and RV260

Objective

The objective of this document is to show you how to configure IPsec Profile for Manual Keying mode on RV160 and RV260 series routers.

Introduction

IPsec ensures that you have secure private communication over the Internet. It gives two or more hosts privacy, integrity, and authenticity for transmitting sensitive information over the Internet. IPsec is commonly used in a Virtual Private Network (VPN), implemented at the IP layer, and can assist many applications that lack security. A VPN is used to provide a secure communication mechanism for sensitive data and IP information that is transmitted through an unsecure network such as the Internet. It provides a flexible solution for remote users and the organization to protect any sensitive information from other parties on the same network.

Manual keying mode reduces the flexibility and options of IPsec. It requires the user to provide the keying material and necessary security association information to each device that is being configured. Manual keying does not scale well as it is usually best used in a small environment.

It is only advisable to use this method if the implementation of Internet Key Exchange (IKE)v1 or IKEv2 on this router is not the same as your remote router or if one of the routers doesn’t support IKE. In these cases, you could manually input the keys. It is recommended to configure auto keying mode for IPsec profile instead of manual keying mode if your router both supports either IKEv1 or IKEv2 and follows the same standards.

When using manual keying mode, make sure that your **Key In** on your local router is the **Key Out** on the remote router and the **Key In** on your remote router is the **Key Out** on your local router.

An example of the configuration for the two routers would be: