User Manual

BCM963XX

IPSec User Guide

963XX-UM201-R

Corporate Headquarters: San Jose, CA

June 16, 2017

For a comprehensive list of changes to this document, see the Revision History.

Table of Contents

Introduction

This document explains how to use the IPSec utility in the WebUI application. The document is aimed at users of the Broadcom CPE reference design boards.

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The IPSec protocol implementation used on the BCM963XX modem is IPSec—Tools (http://ipsec-tools.sourceforge.net/), which is ported from the BSD KAME project (http://www.kame.net/).

Some good references about configuring IPSec from the command line can be found at the following websites:

- The official IPsec How to for Linux— http://www.ipsec-howto.org/
- Linux Advanced Routing and Traffic Control — http://lartc.org/

Linux certificate support is part of OpenSSL. A good reference can be found at:

- OpenSSL Command-Line HOWTO— http://www.madboa.com/geek/openssl

  This implementation supports ESP and AH mode IPSec Tunnel configuration with and without SPU hardware acceleration.

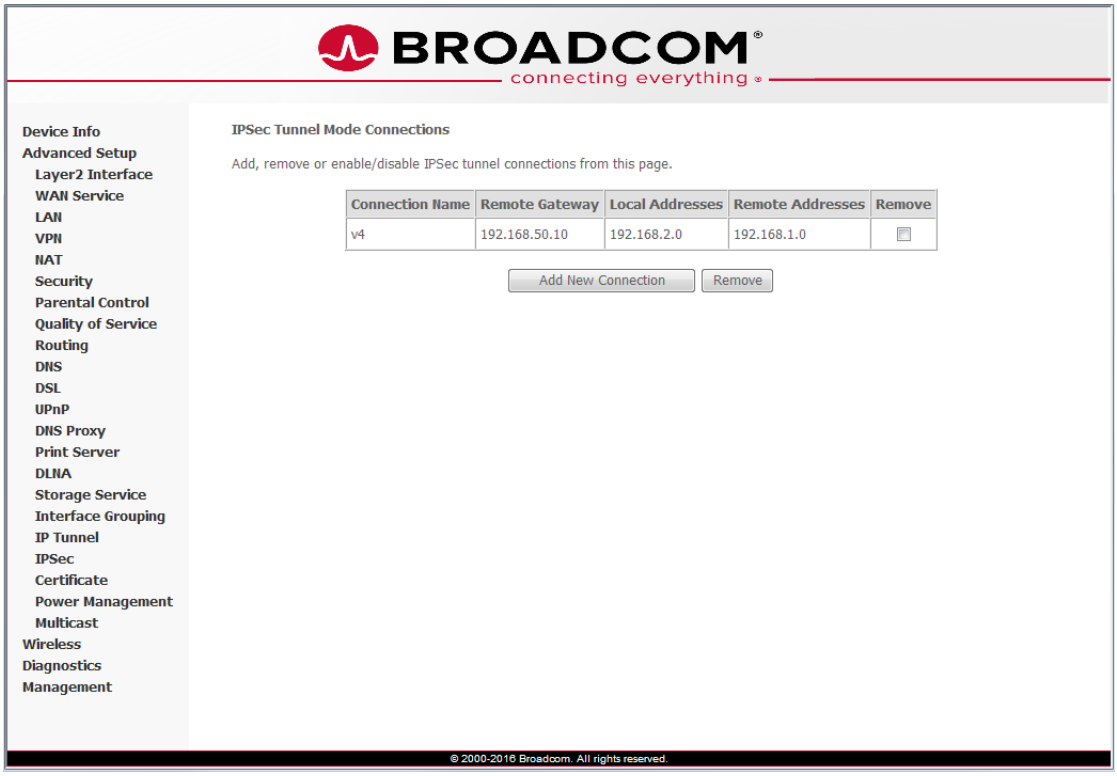
References

Document (or Item) Name	*Number*	*Source*
[1] The official IPsec how to for Linux	–	http://www.ipsec-howto.org/
[2] Linux Advanced Routing and Traffic Control	–	http://lartc.org/
[3] OpenSSL Command-Line How To	–	http://www.madboa.com/geek/openssl

Using IPSec in WebUI

To use IPSec user interface in the WebUI:

1. Open the WebUI of the device.
2. Select **IPSec** from the Advanced Setup menu. The IPSec Tunnel Mode Connections page is displayed.



The table shows the current connections.

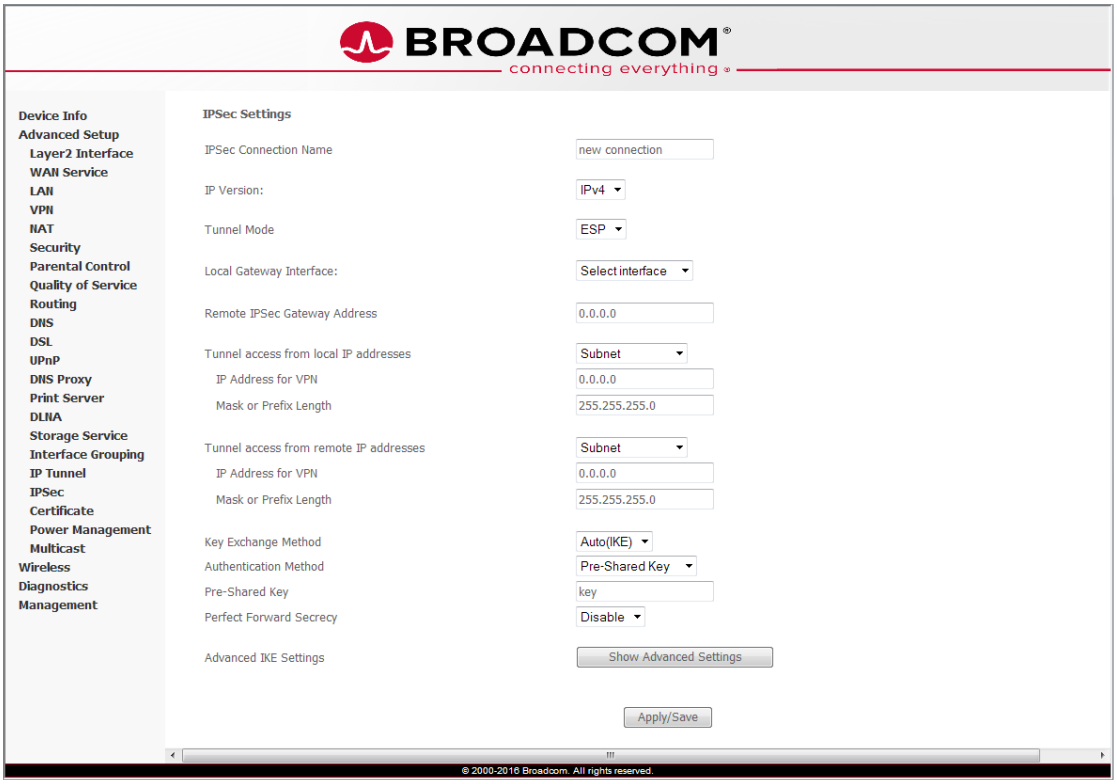
- To remove a connection, use the check box(s) in the Remove column to select one or more connections. Click the **Remove** button to delete the selected connections.
- To add a new connection, click the **Add New Connection** button. See “Adding an IPSec Connection”.

Adding an IPSec Connection

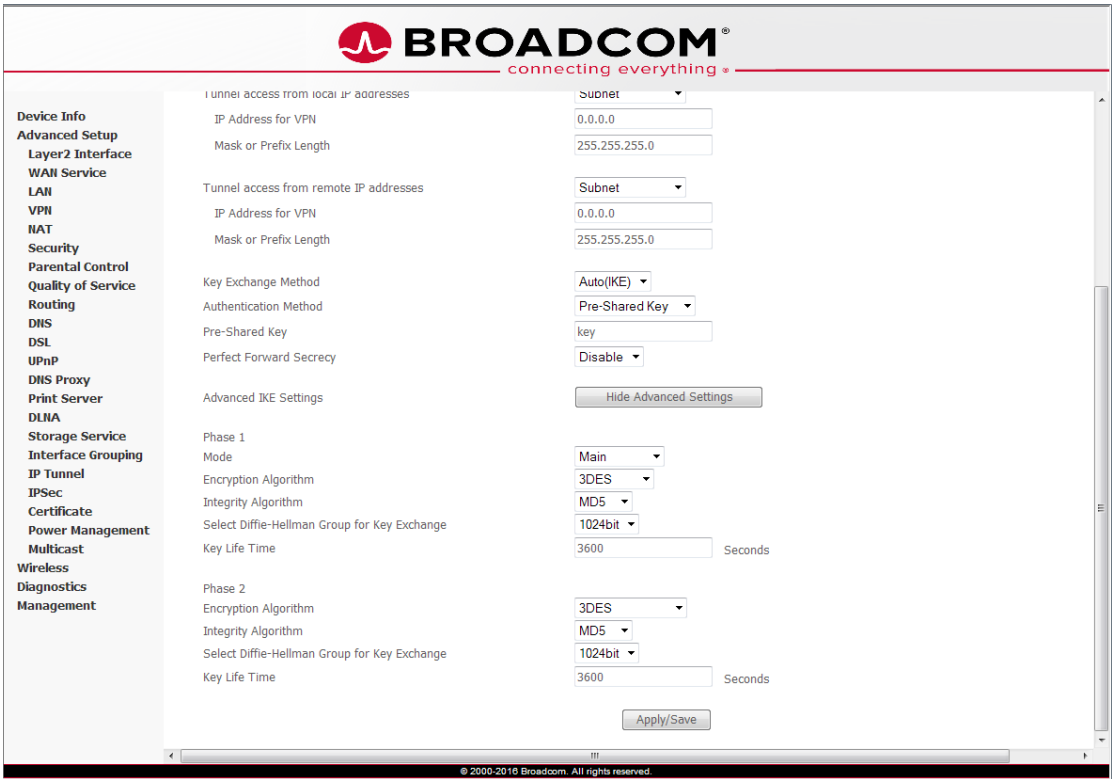
To add an IPSec Connection:

1. From the Main menu, select IPSec to open the IPSec Tunnel Mode Connections page.
2. Click the **Add New Connection** button to open the IPSec Settings page.

   The IPSec Settings page is dynamic. It shows or hides options when different types of connections are selected. The user can select between automatic key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.



3. When automatic key exchange method is used, click **Show Advanced Settings** to show more options, as shown in the following screen.



Using Certificates

To use the Certificate interface, choose **Certificate** under the Advanced Setup menu. There are two menu items under the Certificate menu: “Local” and “CA”. For either type of certificate, the page displays a list of certificates that are stored in the modem.

Under the Certificate menu, “Local” refers to local certificates. “Trusted CA” refers to trusted Certificate Authority certificates. Local certificates preserve the identity of the modem. CA certificates are used by the modem to verify certificates from other hosts.

Local certificates can be created in two ways:

- Create a new certificate request, have it signed by a certificate authority, and load the signed certificate.
- Import an existing signed certificate directly.

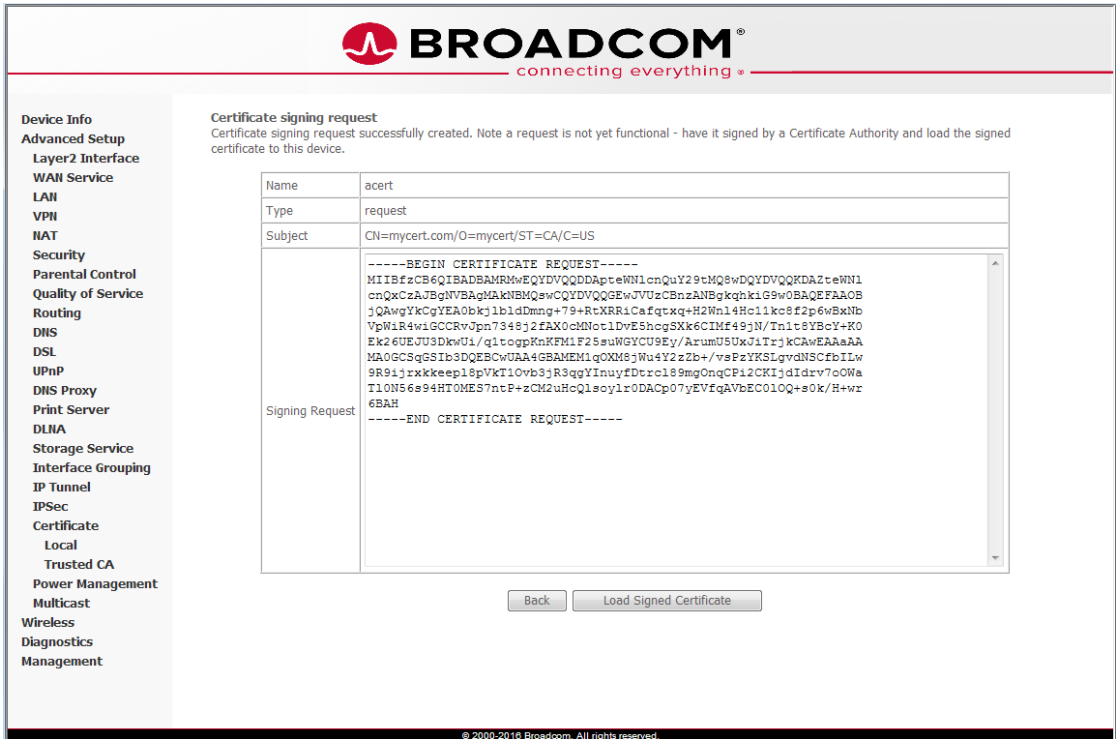
Creating New Certificates

Generating a Certificate

Follow the steps below to create a new certificate.

1. Click **Create Certificate Request** from the Local Certificates page.
2. Enter the necessary information and click **Apply**.

3. After a duration of several seconds, the generated certificate request will be shown.



The certificate request must be submitted to a certificate authority to sign the request. Then the signed certificate must be loaded into the modem. See “Loading a Certificate” on page 10.

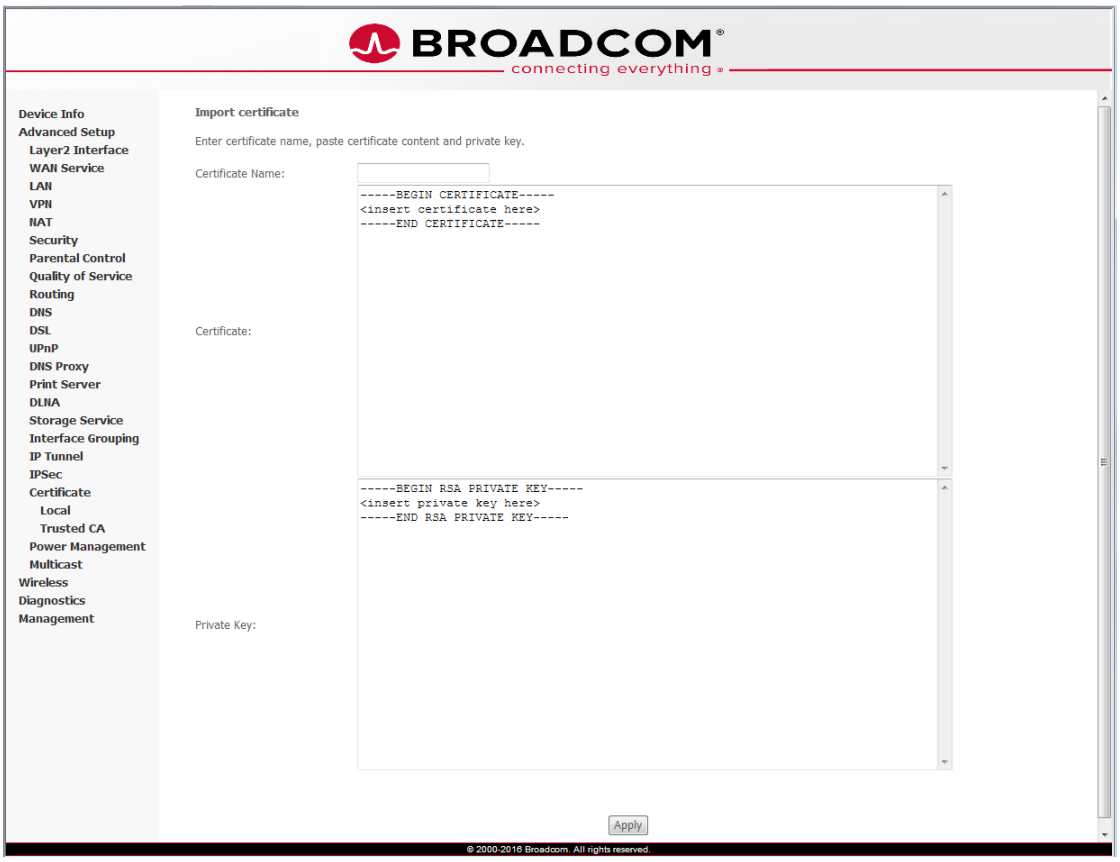
Loading a Certificate

1. Navigate to the Local certificate page, under the Certificate menu, to show the available certificates.
2. Click the **Load Signed** button for the certificate entry you want to update to bring up the load certificate page.
3. Insert the signed certificate into the allocated space, as shown below, and click **Apply**. The new certificate is created.

Importing a Certificate

1. Navigate to the Local Certificate page under the Certificate menu and click the **Import Certificate** button to bring up the Load Certificate page.

2. Insert the certificate and the corresponding private key into the allocated space and click **Apply**.



CA Certificates

A Certificate Authority (CA) certificate can only be imported.

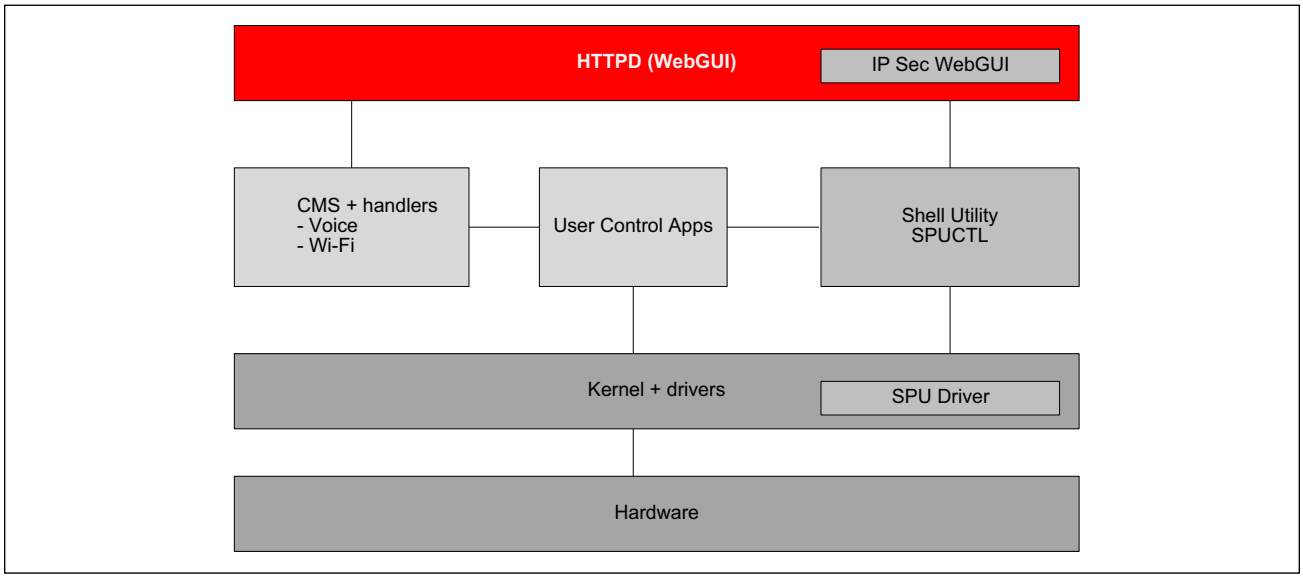
1. Select **Trusted CA** from the Certificate menu. The page for importing the certificate is shown below.
2. Insert the CA certificate in the allocated space and click **Apply**.

SPU Hardware Acceleration

IPSec acceleration is available on enabled devices. In some devices, acceleration is supported via a secure processing unit (SPU), which is a hardware block on the chip.

The architecture of SPU-based IPSec operation is shown in Figure 1. The SPU driver handles complete IPSec packet encryption and hashing, in a single run, asynchronously. When the user configures the first IPSec tunnel, WebUI calls the “spuctl” shell utility to initialize the SPU driver. Then, the SPU driver registers with Linux Crypto API for all the crypto and hash algorithms that it supports. Once this is done, whenever an IPSec packet, either inbound or outbound, comes to the CPE Linux stack, the CPE hands these packets to the SPU Driver for crypto and hash processing.

Figure 1: SPU-based IPSec Operation



Building an IPSec SPU Enabled Image

To build the SPU hardware acceleration feature, follow the steps below:

1. Type **make menuconfig** to open the WebUI.
2. Load the desired profile, for example, 963138GW.
3. Select **WAN Protocols & VPN** from the main menu.
4. Select **SPU Driver** for build-in module.
5. Select **spuctl** as a dynamic build.
6. Save the new profile and build.

By default, SPU is enabled in most of the build profiles that have hardware support. Check this before you modify the parameters.

Flow Cache Support of IPSec Flows Accelerated by SPU

Some of the IPSec flows of “AEAD” type that are accelerated by SPU may also be accelerated by Flow Cache. In order to allow Flow Cache to accelerate these IPSec flows of “AEAD” type, two logical Ethernet interfaces called “spu_ds_dummy” and “spu_us_dummy” get created when the SPU driver is loaded, as illustrated below.

```
# ifconfig
spu_ds_dummy Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0           txqueuelen:100
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

spu_us_dummy Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0           txqueuelen:100
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

As the names of these two logical interfaces suggest, the spu_ds_dummy interface is designated for decrypting the downstream IPSec traffic, whereas the spu_us_dummy interface is designated for encrypting the upstream IPSec traffic. These two logical interfaces serve as the networking endpoints of the SPU hardware block inside the gateway, allowing Flow Cache to accelerate the IPSec packets of interest and deliver them to the SPU via these logical interfaces.

Note: If the spu_ds_dummy and spu_us_dummy logical interfaces cannot be found after the SPU driver is loaded, it implies that Flow Cache acceleration of IPSec flows is not supported in the Broadcom device installed on this gateway.

MTU Settings of spu_ds_dummy and spu_us_dummy

By default, the MTU settings of the two SPU logical interfaces are set to BCM_MAX_MTU_PAYLOAD_SIZE, a system level compile setting which is typically set to 1500. Depending on how the networking interfaces of the gateway are configured, the default MTU settings may NOT be correct and may result in packet fragmentation, which prevents the use of Flow Cache acceleration. To ensure that the IPSec flows of interest get accelerated by Flow Cache, the MTU settings of the SPU logical interfaces must align with the corresponding transmitting interfaces. For instance, in the upstream direction, the SPU logical interface spu_us_dummy's MTU setting shall be the same as the WAN port's MTU setting. Similarly, in the downstream direction, the SPU logical interface spu_ds_dummy's MTU setting shall be the same as the LAN port's MTU setting.

Revision History

Revision	*Date*	*Change Description*
963XX-UM201-R	June 16, 2017	**Updated** • “Building an IPSec SPU Enabled Image” on page 13
963XX-UM200-R	April 20, 2016	Updated from first release 05/04/2010

Web: www.broadcom.com
Corporate Headquarters: San Jose, CA

963XX-UM201-R June 16, 2017