IPSec User Guide

For BCM963xx CPE Linux

Version 1.0

5300 California Avenue • Irvine, CA 92617-7013 USA • Phone: (949) 926-5000 • Fax: (949) 926-5203

Table of Contents

CPE IPSec User Guide

REVISION HISTORY

Revision Number	*Date*	*Change Description*
V1.0	05/04/2010	Initial Release.

1.0 INTRODUCTION

IPSec protocol implementation on the modem is IPSec-Tools (http://ipsec-tools.sourceforge.net/), which is ported from BSD KAME project (http://www.kame.net/).

Good references about IPSec configuration from command line can be found at:

The official IPsec Howto for Linux - http://www.ipsec-howto.org/

Linux Advanced Routing & Traffic Control - http://lartc.org/

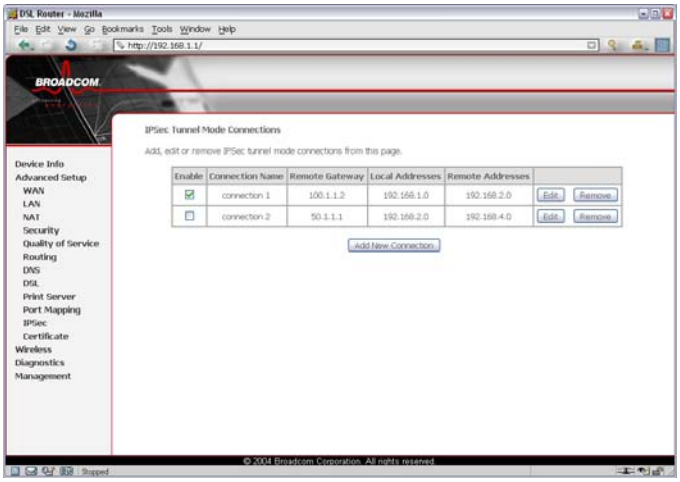
Linux certificate support is part of OpenSSL. A good reference can be found at:

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.

2.0 HOW TO USE IPSEC

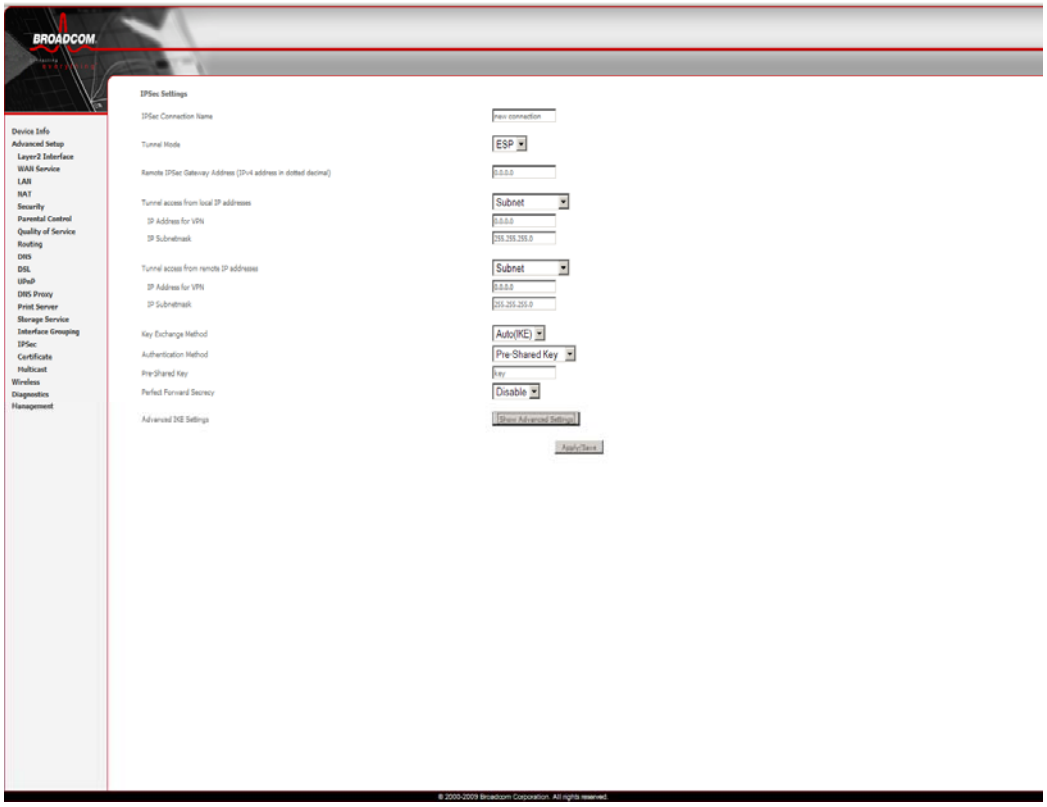
To use IPSec user interface, choose “IPSec” under “Advanced Setup” menu. The base screen will be shown:



The table shows current connections. User can control the following items in the base IPSec page:

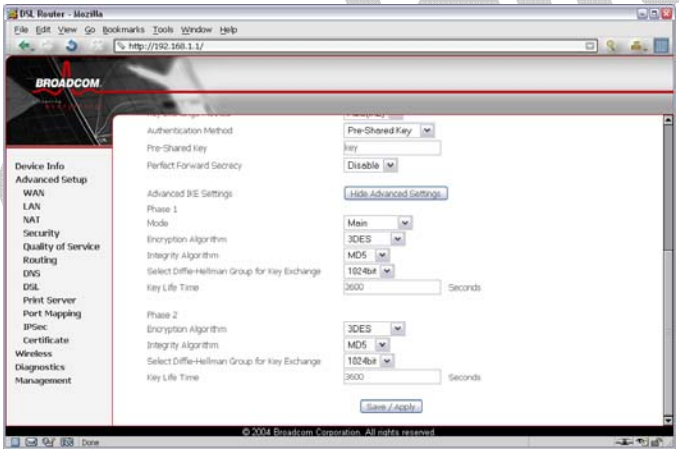
- Click the check box under “Enable” column to enable or disable the connection.
- Click the “Remove” button to remove a connection
- Click the “Add New Connection” button to add a new connection
- Click the “Edit” button to edit a existing connection

The following screen is used to edit configurations when adding or editing an IPSec connection:



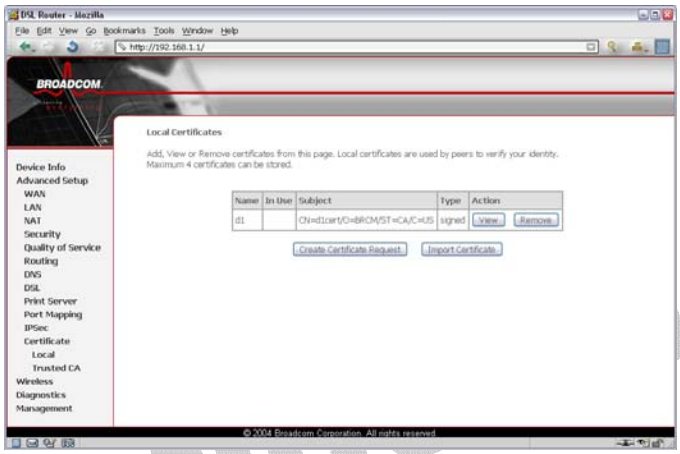
This is a dynamic page. It will change itself by showing and hiding options when different types or connections are chosen. User can select automatic key exchange or manual key exchange, pre-shared key authentication or certificate authentication, etc.

When automatic key exchange method is used, click “Show Advanced Settings” will show more options:



3.0 HOW TO USE CERTIFICATES

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



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

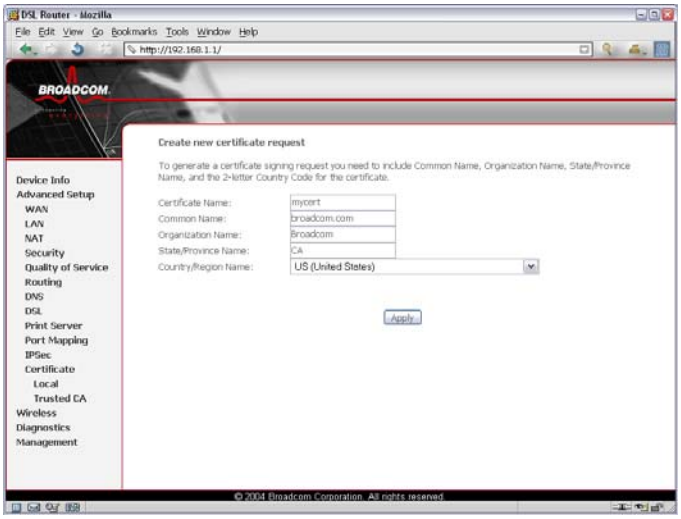
Local certificates can be created by two ways:

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

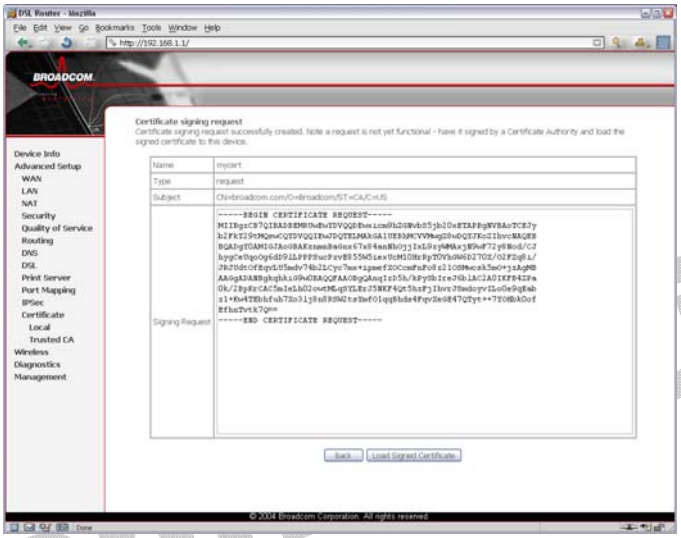
3.1 How to Create New Certificates

Follow the following steps to create a new certificate:

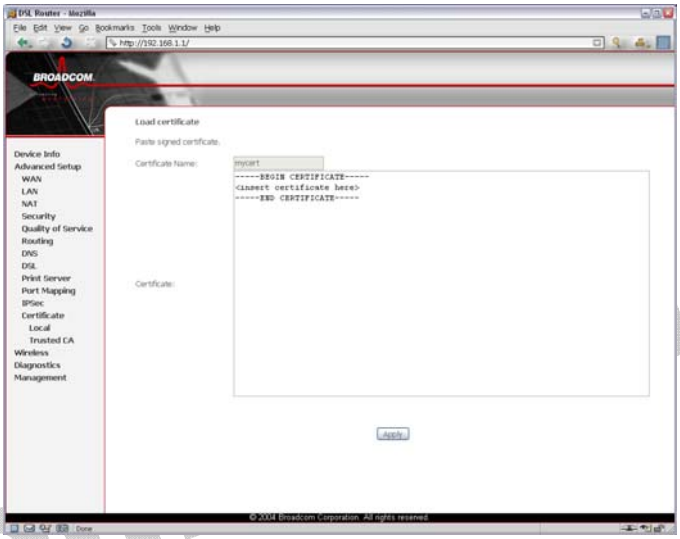
Click “Create Certificate Request”, enter necessary information:



Wait several seconds, the generated certificate request will be shown:

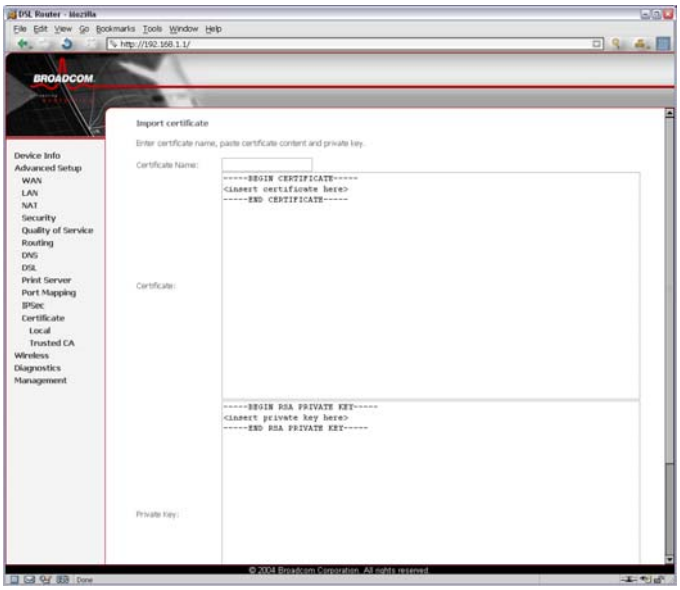


The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click “Load Certificate” button from the previous screen or from the base screen will bring up the load certificate page. Paste the signed certificate and click apply and a new certificate is created.



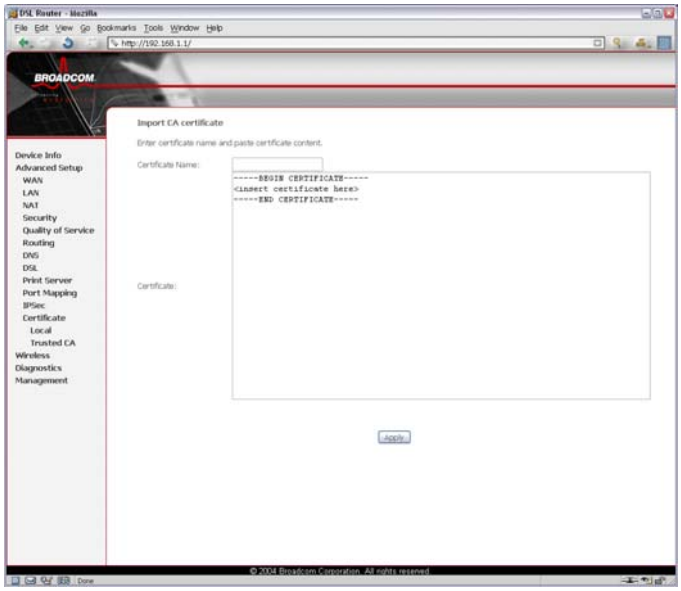
3.2 How to Import Certificates

To import existing certificate, click “Import Certificate” button and paste both certificate and corresponding private key:



3.3 CA Certificates

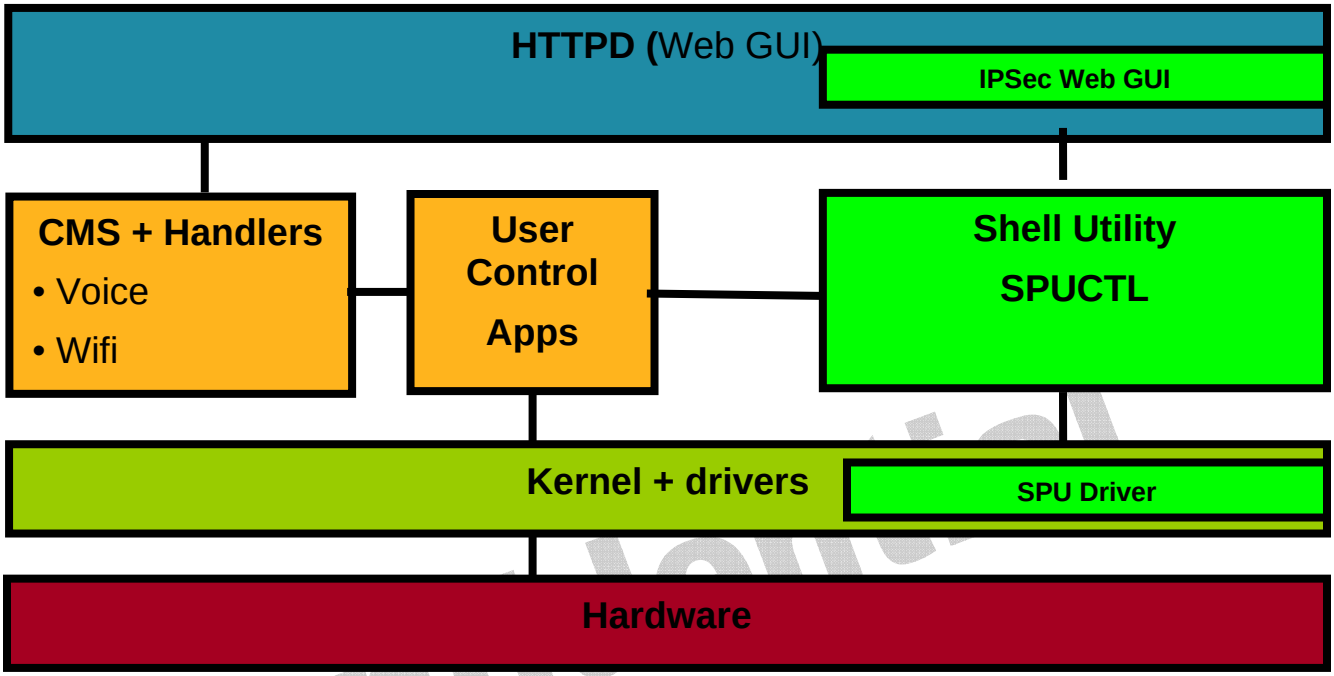
CA certificate can only be imported. The screen for importing is shown below:



4.0 How to Use SPU Hardware Acceleration

Hardware acceleration is supported whenever there exists a SPU hardware block on the chip.

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



5.0 BUILDING IPSEC SPU ENABLED IMAGE

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

Do make menu config

Load 96368GWV profile if you want to build voice image

Go to “WAN Protocols & VPN” section

Select “SPU Driver” for build-in module

Then, select “spuctl” as a dynamic build

Save the new profile and build.

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