



## **IPSec User Guide**

**For BCM963xx CPE Linux**

**Version 1.0**

## ***Table of Contents***

<b>1.0</b>	<b>Introduction.....</b>	<b>2</b>
<b>2.0</b>	<b>How to use IPSec.....</b>	<b>2</b>
<b>3.0</b>	<b>How to Use Certificates .....</b>	<b>4</b>
3.1	How to Create New Certificates.....	4
3.2	How to Import Certificates.....	6
3.3	CA Certificates .....	7
<b>4.0</b>	<b>How to Use SPU Hardware Acceleration.....</b>	<b>7</b>
<b>5.0</b>	<b>Building IPSec SPU Enabled Image.....</b>	<b>8</b>

---

# ***CPE IPSec User Guide***

## **REVISION HISTORY**

<b><i>Revision Number</i></b>	<b><i>Date</i></b>	<b><i>Change Description</i></b>
V1.0	05/04/2010	Initial Release.

This document contains information that is confidential and proprietary to Broadcom<sup>®</sup> Corporation (Broadcom) and may not be reproduced in any form without express written consent of Broadcom. No transfer or licensing of technology is implied by this document. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Copyright © 2005 by Broadcom Corporation. All rights reserved. Printed in the U.S.A.

Broadcom and the pulse logo<sup>®</sup> are trademarks of Broadcom Corporation and/or its subsidiaries in the United States and certain other countries. All other trademarks are the property of their respective owners.

## 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/>

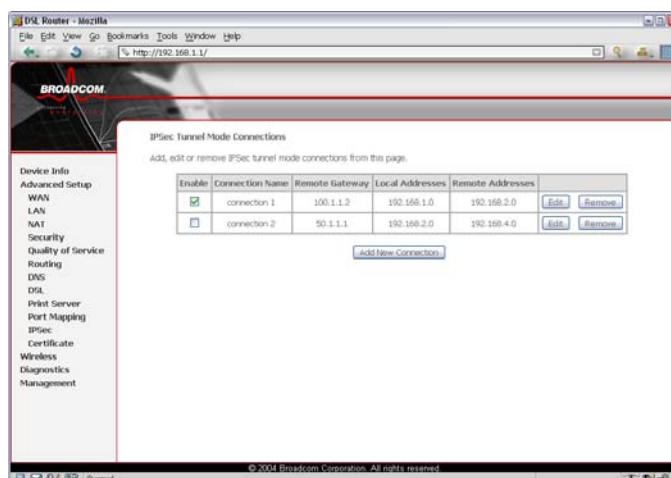
Linux certificate support is part of OpenSSL. A good reference can be found at:

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:

The screenshot shows the 'IPSec Settings' page in a web browser. The left sidebar contains a navigation menu with options: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, DHCP, DNS Proxy, Print Server, Storage Service, Interface Grouping, IPSec, Certificate, Multicast, Wireless, Diagnostics, and Management. The main content area is titled 'IPSec Settings' and includes the following fields and controls:

- IPSec Connection Name:
- Tunnel Mode:
- Remote IPSec Gateway Address (IPv4 address in dotted decimal):
- Tunnel access from local IP address:
- IP Address for VPN:
- IP Subnetmask:
- Tunnel access from remote IP address:
- IP Address for VPN:
- IP Subnetmask:
- Key Exchange Method:
- Authentication Method:
- Pre-Shared Key:
- Perfect Forward Secrecy:
- Show Advanced Settings:
- Apply/Save:

At the bottom of the page, there is a copyright notice: © 2000-2009 Broadcom Corporation. All rights reserved.

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:

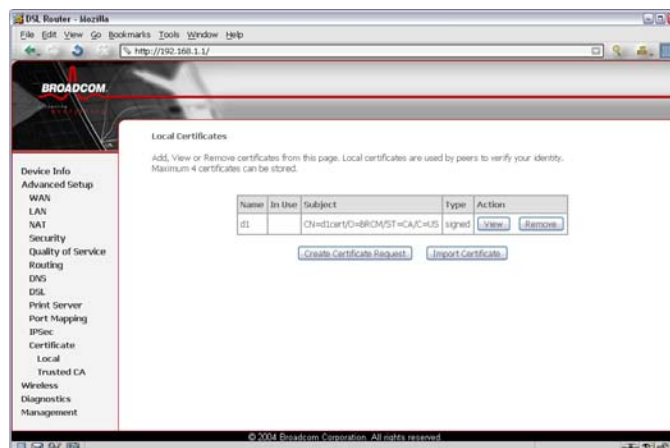
The screenshot shows the 'IPSec Settings' page with the 'Show Advanced Settings' button clicked. The main content area now displays additional configuration options:

- Authentication Method:
- Pre-Shared Key:
- Perfect Forward Secrecy:
- Advanced IKE Settings:
- Phase 1:
  - Mode:
  - Encryption Algorithm:
  - Integrity Algorithm:
  - Select Diffie-Hellman Group for Key Exchange:
  - Key Life Time:  Seconds
- Phase 2:
  - Encryption Algorithm:
  - Integrity Algorithm:
  - Select Diffie-Hellman Group for Key Exchange:
  - Key Life Time:  Seconds
- Save/Apply:

At the bottom of the page, there is a copyright notice: © 2004 Broadcom Corporation. All rights reserved.

## 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 verify certificates from other hosts.

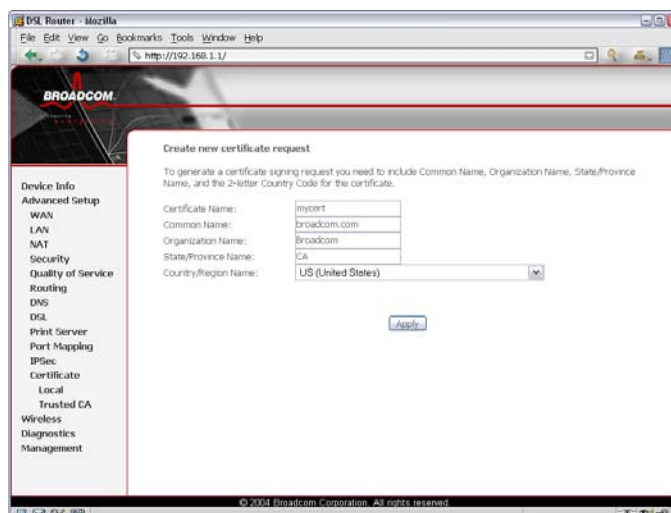
Local certificates can be created by two ways:

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

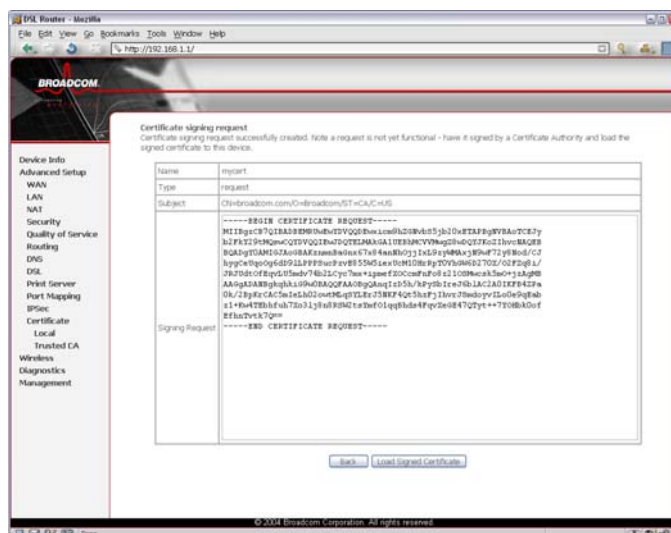
### 3.1 How to Create New Certificates

Follow the following steps to create a new certificate:

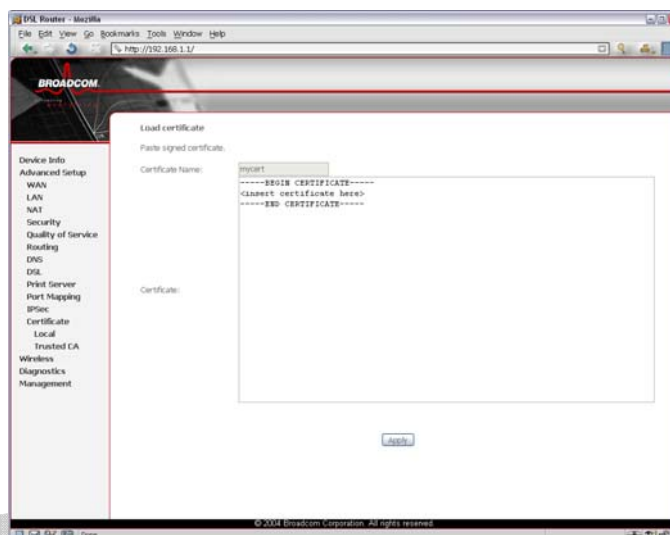
Click “Create Certificate Request”, enter necessary information:



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

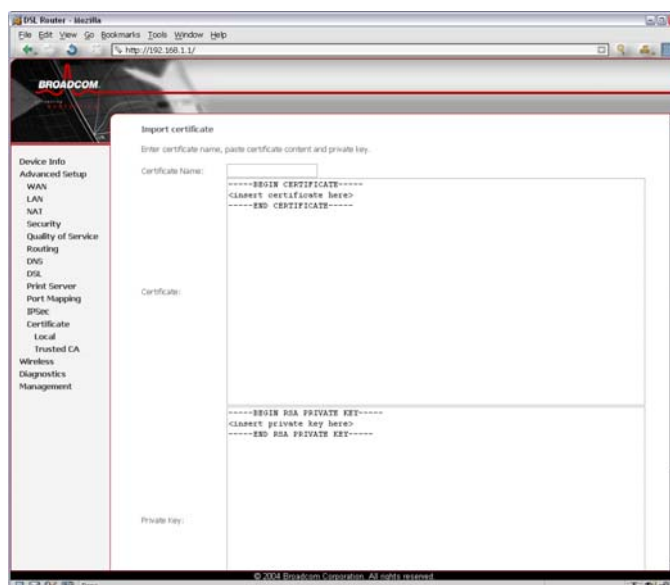


The certificate request needs to be submitted to a certificate authority, which would sign the request. Then the signed certificate needs to be loaded into modem. Click “Load Certificate” button from the previous screen or from the base screen will bring up the load certificate page. Paste the signed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



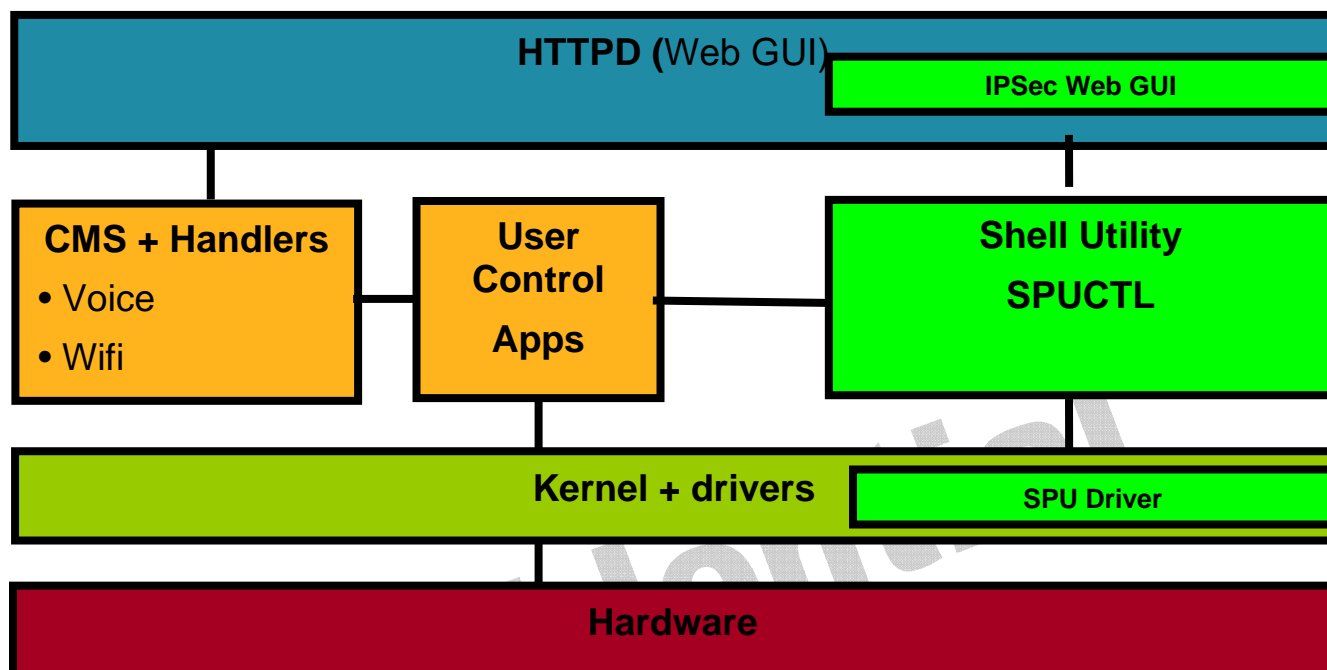
### 3.2 How to Import Certificates

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









## 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.