

IPSec User Guide

For a comprehensive list of changes to this document, see the [Revision History](#).

Broadcom, the pulse logo, Connecting everything, Avago, Avago Technologies, and the A logo are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries and/or the EU.

Copyright © 2016–2017 by Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Limited and/or its subsidiaries. For more information, please visit www.broadcom.com.

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.

Table of Contents

- Introduction**..... 4
 - References 4
- Using IPSec in WebUI** 5
 - Adding an IPSec Connection 6
- Using Certificates** 8
 - Creating New Certificates..... 8
 - Generating a Certificate 8
 - Loading a Certificate 10
 - Importing a Certificate 11
 - CA Certificates 12
- SPU Hardware Acceleration** 13
- Revision History** 15

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.

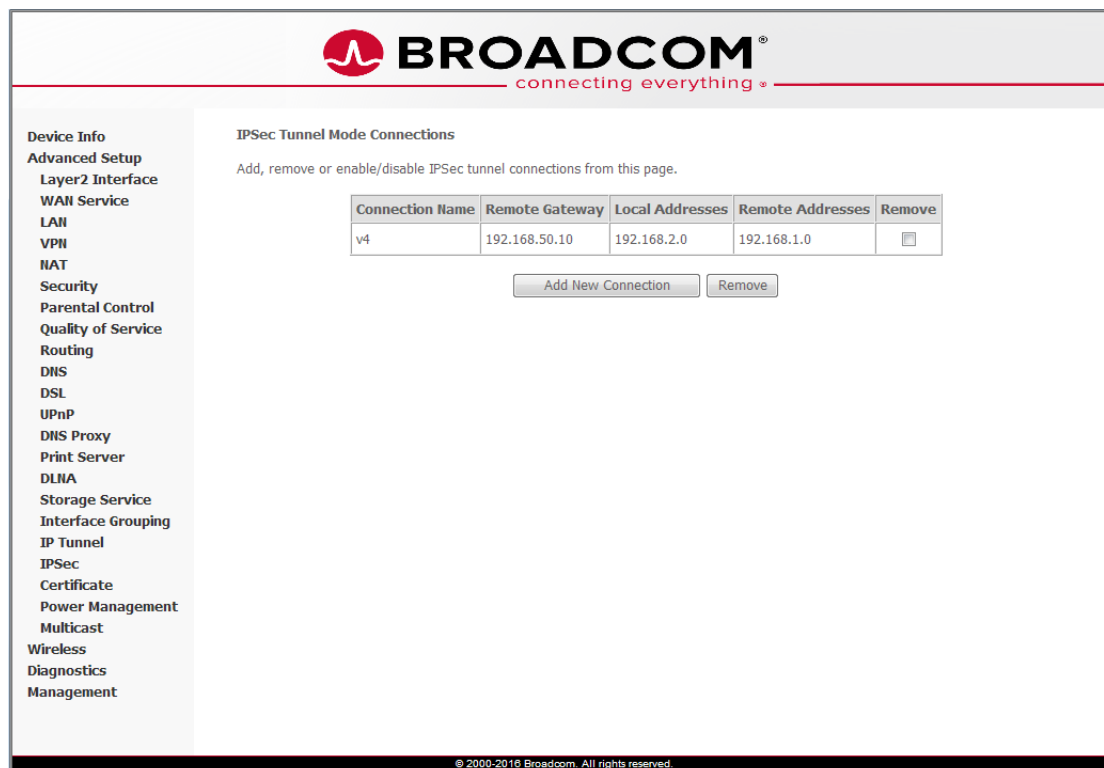
References

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



BROADCOM
connecting everything

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
VPN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Power Management
Multicast
Wireless
Diagnostics
Management

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
v4	192.168.50.10	192.168.2.0	192.168.1.0	<input type="checkbox"/>

Add New Connection Remove

© 2000-2016 Broadcom. All rights reserved.

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:

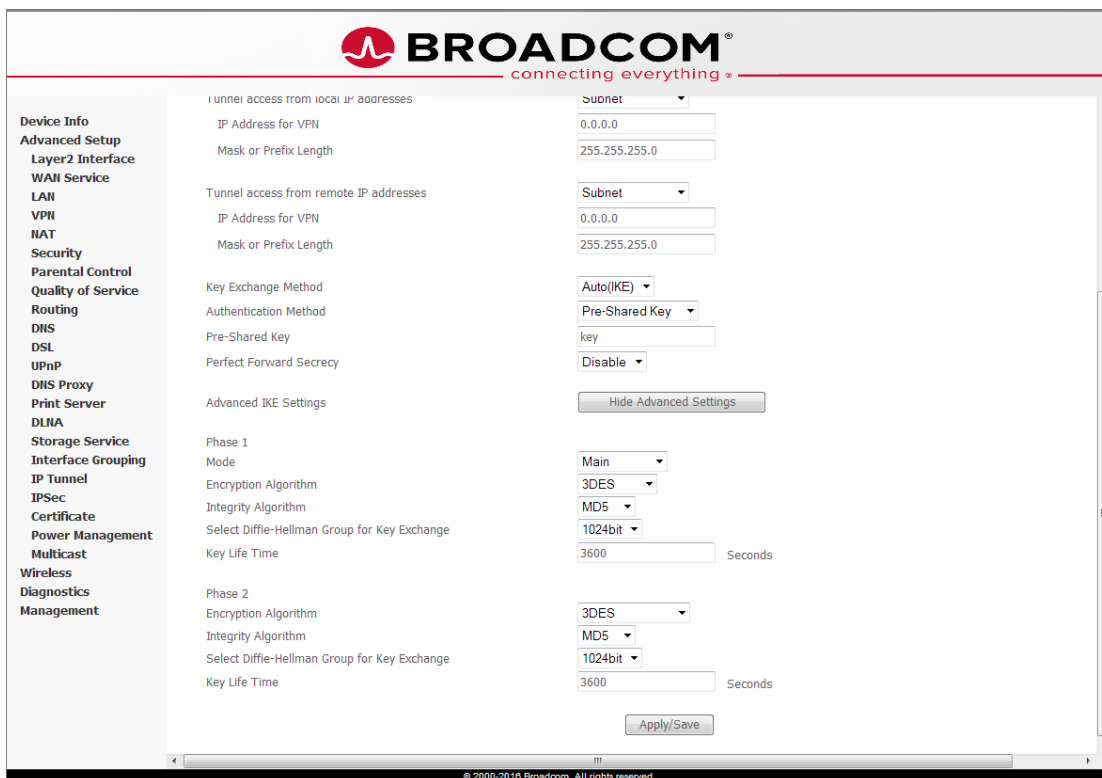
1. From the Main menu, select IPSec to open the IPSec Tunnel Mode Connections page.
2. Click the **Add New Connection** button to open the IPSec Settings page.

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.

The screenshot displays the Broadcom web interface for configuring an IPSec connection. The top header features the Broadcom logo and the tagline "connecting everything". A left-hand navigation menu lists various system settings categories, with "IPSec" currently selected. The main content area, titled "IPSec Settings", contains several configuration fields and dropdown menus. The "IPSec Connection Name" field is set to "new connection". The "IP Version" is set to "IPv4", and the "Tunnel Mode" is set to "ESP". The "Local Gateway Interface" is set to "Select interface". The "Remote IPSec Gateway Address" is set to "0.0.0.0". The "Tunnel access from local IP addresses" is set to "Subnet", with the "IP Address for VPN" set to "0.0.0.0" and the "Mask or Prefix Length" set to "255.255.255.0". The "Tunnel access from remote IP addresses" is also set to "Subnet", with the "IP Address for VPN" set to "0.0.0.0" and the "Mask or Prefix Length" set to "255.255.255.0". The "Key Exchange Method" is set to "Auto(IKE)", the "Authentication Method" is set to "Pre-Shared Key", and the "Pre-Shared Key" field contains the text "key". The "Perfect Forward Secrecy" is set to "Disable". A "Show Advanced Settings" button is located below the "Perfect Forward Secrecy" field. At the bottom of the form is an "Apply/Save" button. The footer of the page indicates the copyright "© 2000-2015 Broadcom. All rights reserved."

IPSec Settings	
IPSec Connection Name	new connection
IP Version:	IPv4
Tunnel Mode	ESP
Local Gateway Interface:	Select interface
Remote IPSec Gateway Address	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
Mask or Prefix Length	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
Mask or Prefix Length	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Show Advanced Settings
Apply/Save	

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



BROADCOM
connecting everything

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
VPN
NAT
Security
Parental Control
Quality of Service
Routing
DHCP
DSL
UPnP
DNS Proxy
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Power Management
Multicast
Wireless
Diagnostics
Management

Tunnel access from local IP addresses

Subnet
IP Address for VPN
Mask or Prefix Length

Tunnel access from remote IP addresses

Subnet
IP Address for VPN
Mask or Prefix Length

Key Exchange Method
Authentication Method
Pre-Shared Key
Perfect Forward Secrecy

Auto(IKE)
Pre-Shared Key
key
Disable

Hide Advanced Settings

Advanced IKE Settings

Phase 1
Mode
Encryption Algorithm
Integrity Algorithm
Select Diffie-Hellman Group for Key Exchange
Key Life Time

Main
3DES
MD5
1024bit
3600 Seconds

Phase 2
Encryption Algorithm
Integrity Algorithm
Select Diffie-Hellman Group for Key Exchange
Key Life Time

3DES
MD5
1024bit
3600 Seconds

Apply/Save

© 2000-2016 Broadcom. All rights reserved.

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

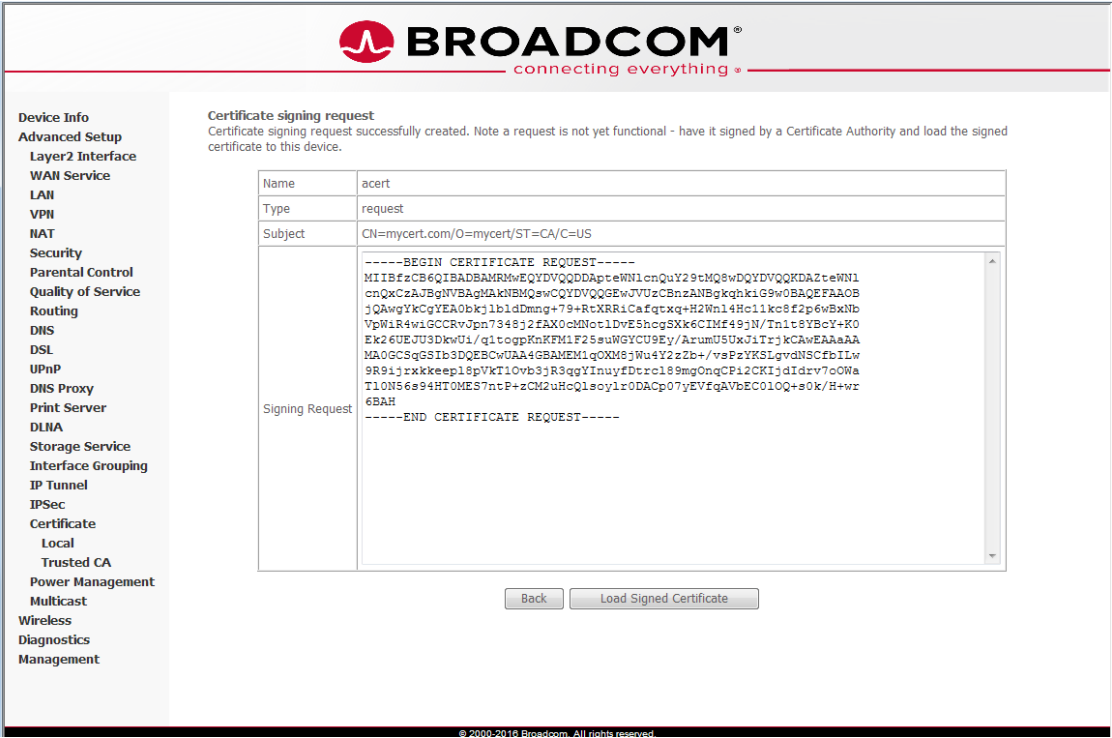
Generating a Certificate

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**.

The screenshot shows the Broadcom modem web interface. The top header features the Broadcom logo and the tagline "connecting everything". On the left is a navigation menu with categories like Device Info, Advanced Setup, WAN Service, LAN, VPN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, Print Server, DLNA, Storage Service, Interface Grouping, IP Tunnel, IPSec, Certificate, Local, Trusted CA, Power Management, Multicast, Wireless, Diagnostics, and Management. The main content area is titled "Create new certificate request" and includes instructions: "To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate." Below this are input fields for Certificate Name (acert), Common Name (mycert.com), Organization Name (mycert), State/Province Name (CA), and Country/Region Name (US (United States)). An "Apply" button is located at the bottom right of the form. The footer of the page reads "© 2000-2016 Broadcom. All rights reserved."

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](#).

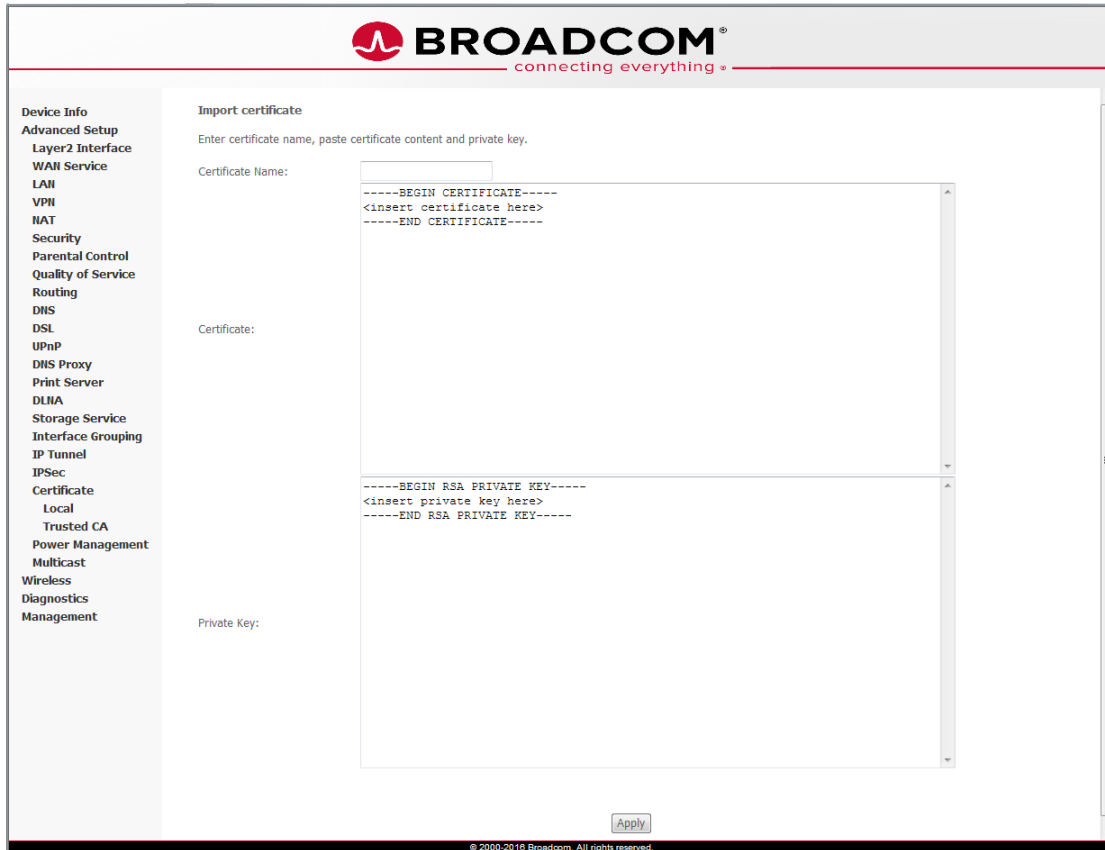
Loading a Certificate

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.

The screenshot shows the Broadcom web interface. At the top is the Broadcom logo with the tagline "connecting everything". On the left is a navigation menu with categories: Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, VPN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, Print Server, DLNA, Storage Service, Interface Grouping, IP Tunnel, IPSec, Certificate, Local, Trusted CA, Power Management, Multicast, Wireless, Diagnostics, and Management. The "Certificate" menu item is selected. The main content area is titled "Load certificate" and contains the instruction "Paste signed certificate.". Below this, there is a "Certificate Name:" label followed by a text input field containing "acert". To the right of the input field is a large text area for pasting the certificate, which contains the placeholder text: "-----BEGIN CERTIFICATE-----", "<insert certificate here>", and "-----END CERTIFICATE-----". Below the text area is an "Apply" button. At the bottom of the page, there is a small copyright notice: "© 2000-2016 Broadcom. All rights reserved."

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**.



BROADCOM
connecting everything

Device Info
Advanced Setup
Layer2 Interface
WAN Service
LAN
VPN
NAT
Security
Parental Control
Quality of Service
Routing
DNS
DSL
UPnP
DNS Proxy
Print Server
DLNA
Storage Service
Interface Grouping
IP Tunnel
IPSec
Certificate
Local
Trusted CA
Power Management
Multicast
Wireless
Diagnostics
Management

Import certificate
Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Private Key:

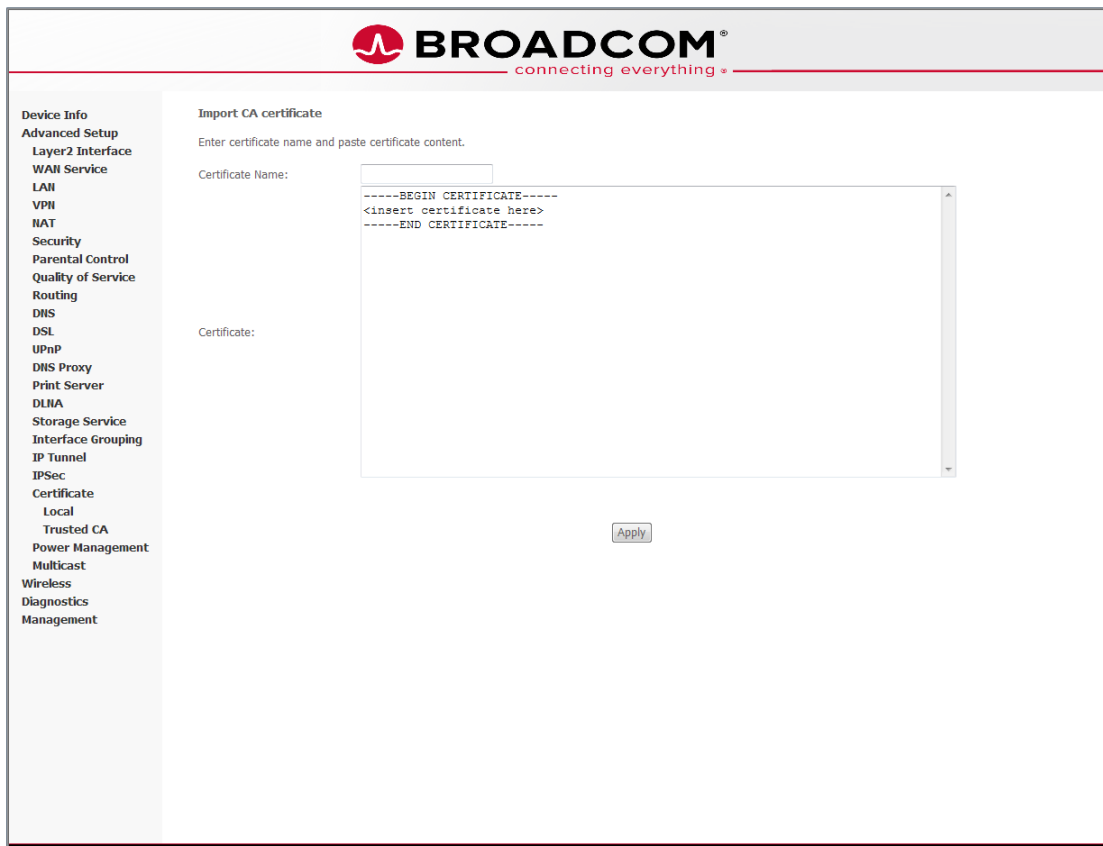
```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```

© 2000-2016 Broadcom. All rights reserved.

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**.



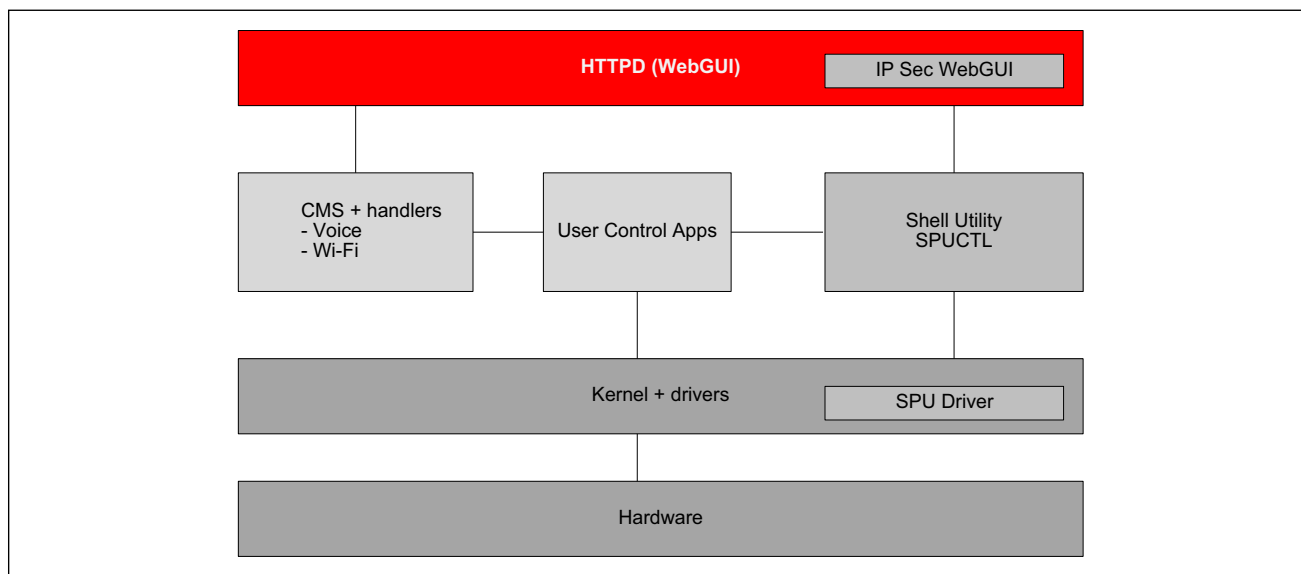
The screenshot shows the Broadcom web interface for importing a CA certificate. The Broadcom logo is at the top center. On the left is a navigation menu with categories like Device Info, Advanced Setup, Layer2 Interface, WAN Service, LAN, VPN, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, UPnP, DNS Proxy, Print Server, DLNA, Storage Service, Interface Grouping, IP Tunnel, IPSec, Certificate, Local, Trusted CA, Power Management, Multicast, Wireless, Diagnostics, and Management. The 'Trusted CA' option is selected. The main content area is titled 'Import CA certificate' and contains the instruction 'Enter certificate name and paste certificate content.' There is a 'Certificate Name:' label next to a text input field. Below it is a large text area for the certificate content, which contains the placeholder text: '-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----'. At the bottom right of the main content area is an 'Apply' button. The footer of the page contains the copyright notice '© 2009-2016 Broadcom. All rights reserved.'

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

<i>Revision</i>	<i>Date</i>	<i>Change Description</i>
963XX-UM201-R	June 16, 2017	Updated <ul style="list-style-type: none">• “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

© 2016–2017 by Broadcom. All rights reserved.

963XX-UM201-R June 16, 2017