

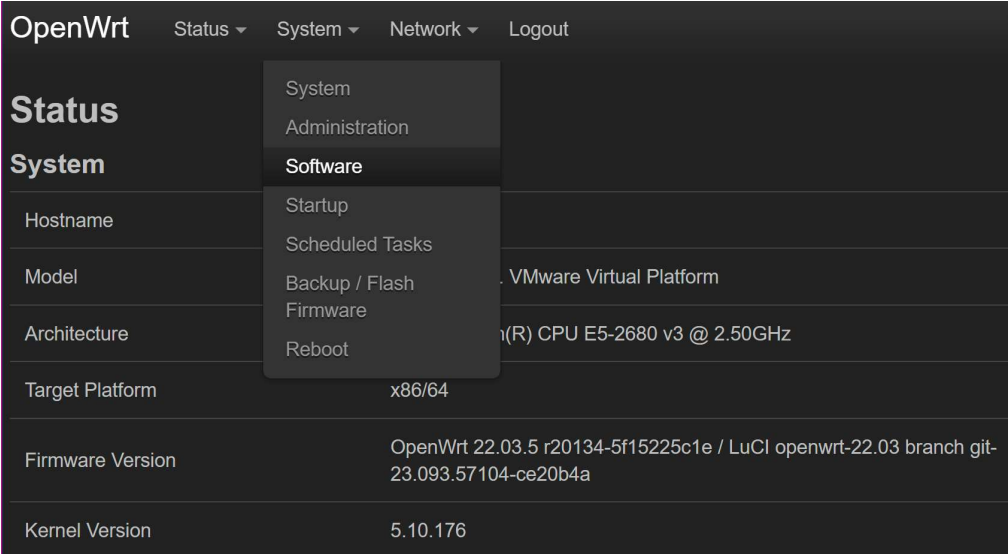
# Openconnect

2023年12月28日 10:51

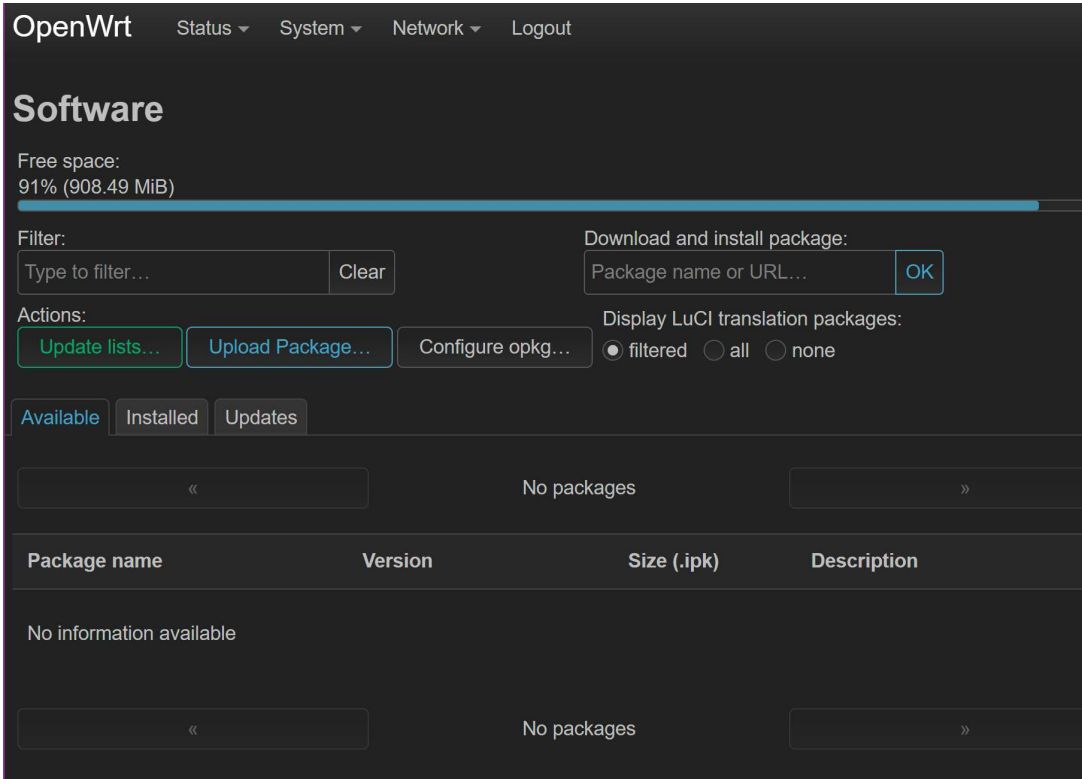
Ocserv 的client  
我用的openwrt 22.03, 其他版本应该也可以

## Part A: 安装openconnect:

1. 点Menu下的System --> Software



2. 点击update lists (更新软件仓库的软件列表)



成功后是这个样子：很多Updated list of ... (成功更新...)

**Executing package manager**

```
Downloading
https://downloads.openwrt.org/releases/22.03.5/targets/x86/64/packages/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_core
Downloading
https://downloads.openwrt.org/releases/22.03.5/targets/x86/64/packages/Packages.sig
Signature check passed.
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/base/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_base
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/base/Packages.sig
Signature check passed.
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/luci/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_luci
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/luci/Packages.sig
Signature check passed.
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_packages
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/Packages.sig
Signature check passed.
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/routing/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_routing
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/routing/Packages.sig
Signature check passed.
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/telephony/Packages.gz
Updated list of available packages in /var/opkg-lists/openwrt_telephony
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/telephony/Packages.sig
Signature check passed.
```

Dismiss

- 成功更新后你的available tab就不是空的了. 在filter 中填入 openconnect, 只显示 openconnect相关的.

OpenWrt
Status
System
Network
Logout

## Software

Free space:  
91% (913.18 MiB)

Filter:
Clear

Download and install package:
OK

Actions:

Display LuCI translation packages:
☒ filtered
☐ all
☐ none

«
Displaying 1-4 of 4
»

| Package name                           | Version                  | Size (.ipk) | Description                                                                                                    |
|----------------------------------------|--------------------------|-------------|----------------------------------------------------------------------------------------------------------------|
| <a href="#">openconnect</a>            | 9.01-1                   | 172.75 KiB  | A VPN client compatible with several SSL VPN implementations (ocserv, Cisco AnyConnect, Juniper, Palo Alto)... |
| <a href="#">luci-app-ocserv</a>        | git-20.110.55046-74da73b | 5.35 KiB    | LuCI Support for <a href="#">OpenConnect</a> VPN                                                               |
| <a href="#">luci-proto-openconnect</a> | git-23.093.42704-230ba69 | 3.51 KiB    | Support for <a href="#">OpenConnect</a> VPN                                                                    |
| <a href="#">ocserv</a>                 | 1.1.6-2                  | 256.16 KiB  | <a href="#">OpenConnect</a> server (ocserv) is an SSL VPN server. Its purpose is to be...                      |

«
Displaying 1-4 of 4
»

有个叫luci-proto-openconnect，点它右边的install.

(只安装它就可以了. 安装它会同时安装它所依赖的openconnect. ocserv (openconnect server)不用安装, 除非你想从外网(商场的免费WIFI)连到自己家的内网.)

Details for package *luci-proto-openconnect*

Version: git-23.093.42704-230ba69

Size: ~2.69 KiB installed

Dependencies:

↳ openconnect (171.71 KiB) NOT INSTALLED

↳ libxml2 (497.15 KiB) NOT INSTALLED

↳ libpthread INSTALLED

↳ libgcc1 INSTALLED

↳ zlib INSTALLED

↳ kmod-tun (23.75 KiB) NOT INSTALLED

↳ kernel INSTALLED

↳ resolveip (1.63 KiB) NOT INSTALLED

↳ vpnc-scripts (2.23 KiB) NOT INSTALLED

↳ libgnutls (885.78 KiB) NOT INSTALLED

↳ libnettle8 (316.03 KiB) NOT INSTALLED

↳ libgmp10 (208.75 KiB) NOT INSTALLED

↳ libatomic1 (6.94 KiB) NOT INSTALLED

↳ libtasn1 (30.64 KiB) NOT INSTALLED

Description

Support for OpenConnect VPN

Require approx. 2.10 MiB size for 11 package(s) to install.

☐ Allow overwriting conflicting package files

Cancel

Install

没出什么错, 这样就安装好了.  
安装好了后, 重启openwrt

OpenWRT Page 4

```

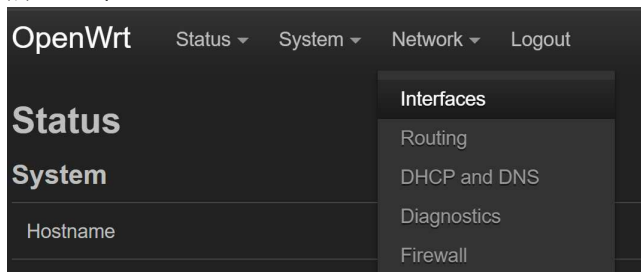
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/libxml
12_2.10.4-1_x86_64.ipk
Installing kmod-tun (5.10.176-1) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/targets/x86/64/packages/kmod-
tun_5.10.176-1_x86_64.ipk
Installing resolveip (2) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/base/resolveip
_2_x86_64.ipk
Installing vpnc-scripts (20151220-2) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/vpnc-
scripts_20151220-2_all.ipk
Installing libgmp10 (6.2.1-1) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/base/libgmp10_
6.2.1-1_x86_64.ipk
Installing libnettle8 (3.7.3-2) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/base/libnettle
8_3.7.3-2_x86_64.ipk
Installing libatomic1 (11.2.0-4) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/targets/x86/64/packages/libato
mic1_11.2.0-4_x86_64.ipk
Installing libgnutls (3.7.1-2) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/libgn
utls_3.7.1-2_x86_64.ipk
Installing libtasn1 (4.16.0-2) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/libta
asn1_4.16.0-2_x86_64.ipk
Installing openconnect (9.01-1) to root...
Downloading
https://downloads.openwrt.org/releases/22.03.5/packages/x86_64/packages/openc
onnect_9.01-1_x86_64.ipk
Configuring libxml2.
Configuring kmod-tun.
Configuring resolveip.
Configuring vpnc-scripts.
Configuring libgmp10.
Configuring libnettle8.
Configuring libatomic1.
Configuring libgnutls.
Configuring libtasn1.
Configuring openconnect.
Configuring luci-proto-openconnect.

```

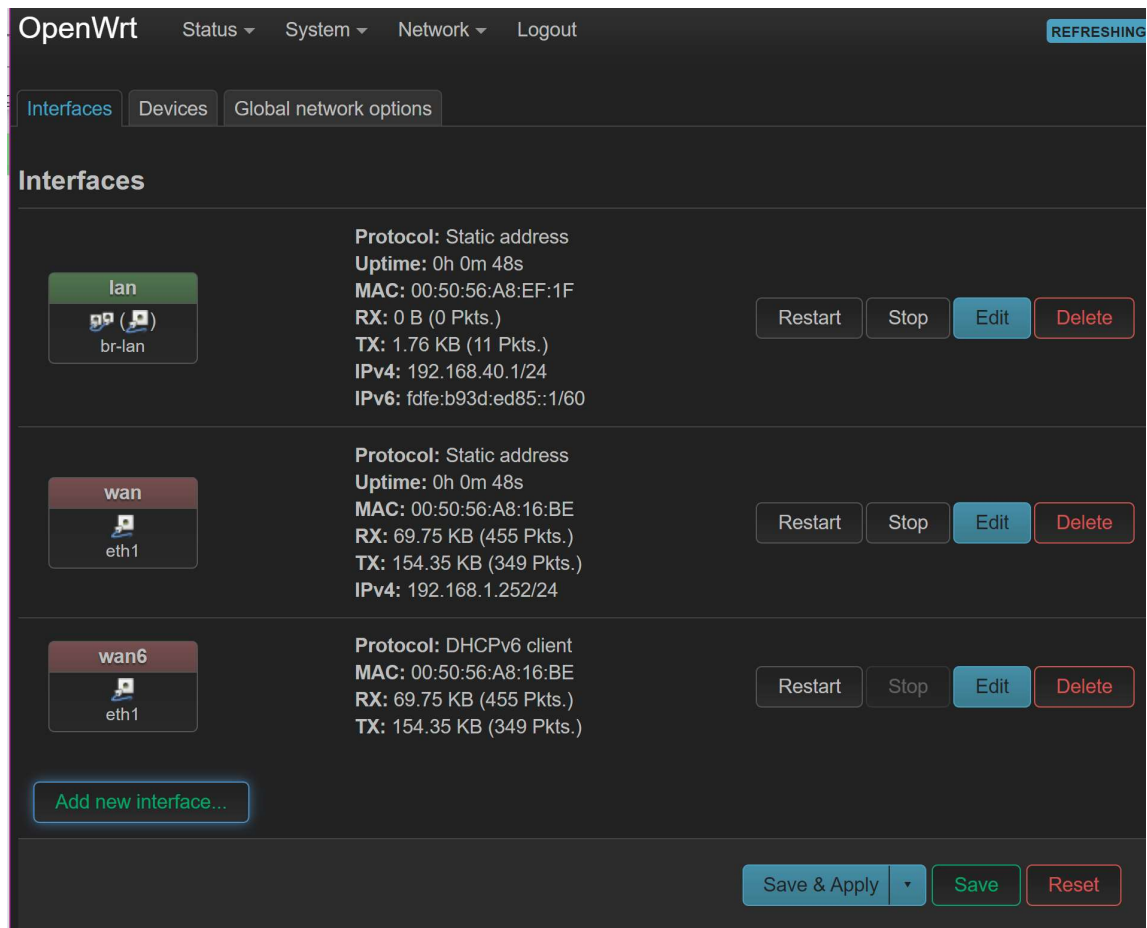
Dismiss

## Part B: 设置openconnect

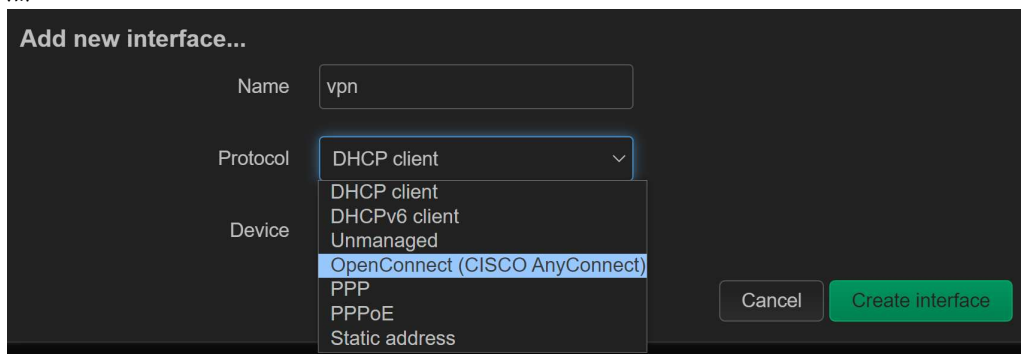
### 1. 点Menu 下 Network --> Interfaces



### 2. 点 Add new interface



- name随便取个名字, 这里用的是vpn, Protocol 选OpenConnect (CISCO AnyConnect), 点Create interface



- 填几项就可以了:  
 VPN Server (域名或ip都行)  
 VPN Server port (端口 我用的缺省443)  
 Username (用户名)  
 Password (密码)  
 填完上表后,点save

Interfaces » vpn


General Settings

Advanced Settings

Firewall Settings

DHCP Server

Status

 Device: openconnect-vpn  
RX: 0 B (0 Pkts.)  
TX: 0 B (0 Pkts.)

Protocol

OpenConnect (CISCO AnyCon ▾)

Bring up on boot

☒

VPN Protocol

Cisco AnyConnect SSL VPN ▾

VPN Server

VPN Server port

443

VPN Server's certificate SHA1 hash

Auth Group

User Group

Username

Password





\*

Password2

\*

5. 填完上表后,点save 跳转到这个页面, 点Save & Apply


## Interfaces

|                                                                                                                    |                                                                                                                                                                                                                                 |                          |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b>lan</b><br><br>br-lan          | <b>Protocol:</b> Static address<br><b>Uptime:</b> 0h 55m 19s<br><b>MAC:</b> 00:50:56:A8:EF:1F<br><b>RX:</b> 0 B (0 Pkts.)<br><b>TX:</b> 3.33 KB (20 Pkts.)<br><b>IPv4:</b> 192.168.40.1/24<br><b>IPv6:</b> fdfe:b93d:ed85::1/60 | Restart Stop Edit Delete |
| <b>vpn</b><br><br>openconnect-vpn | <b>Protocol:</b> OpenConnect (CISCO AnyConnect)<br><b>Interface has 6 pending changes</b>                                                                                                                                       | Restart Stop Edit Delete |
| <b>wan</b><br><br>eth1            | <b>Protocol:</b> Static address<br><b>Uptime:</b> 0h 55m 19s<br><b>MAC:</b> 00:50:56:A8:16:BE<br><b>RX:</b> 963.24 KB (9491 Pkts.)<br><b>TX:</b> 732.65 KB (1417 Pkts.)<br><b>IPv4:</b> 192.168.1.252/24                        | Restart Stop Edit Delete |
| <b>wan6</b><br><br>eth1           | <b>Protocol:</b> DHCPv6 client<br><b>MAC:</b> 00:50:56:A8:16:BE<br><b>RX:</b> 963.24 KB (9491 Pkts.)<br><b>TX:</b> 732.65 KB (1417 Pkts.)                                                                                       | Restart Stop Edit Delete |

Add new interface...

Save & Apply Save Reset

6. IPv4 有地址(因服务器设置而异, 我的是10.10.10.0 网段), RX, TX有数据包, 就是连上服务器了. 路由器自身可以自由上网了.


|                                                                                                              |                                                                                                                                                                                                                                   |                          |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b>vpn</b><br><br>vpn-vpn | <b>Protocol:</b> OpenConnect (CISCO AnyConnect)<br><b>Uptime:</b> 0h 0m 23s<br><b>RX:</b> 640 B (9 Pkts.)<br><b>TX:</b> 304 B (4 Pkts.)<br><b>IPv4:</b> 10.10.10.39/32<br><b>IPv6:</b> fda9:4efe:7e3b:1c24:fce:6921:dc49:7a4b/128 | Restart Stop Edit Delete |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|

7. 电脑手机如果如果想通过这个路由器上网, 还要设一下防火墙  
Menu --> Network --> Firewall

OpenWrt Status System Network Logout

Interfaces Devices Global network o

## Interfaces

|                                                                                                             |                                                                                                                                                                                                                                              |                          |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b>lan</b><br><br>br-lan | <b>Protocol:</b> Static address<br><b>Uptime:</b> 0h 55m 19s<br><b>MAC:</b> 00:50:56:A8:EF:1F<br><b>RX:</b> 518.88 KB (4450 Pkts.)<br><b>TX:</b> 312.08 KB (3852 Pkts.)<br><b>IPv4:</b> 192.168.40.1/24<br><b>IPv6:</b> fdfe:b93d:ed85::1/60 | Restart Stop Edit Delete |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|

Interfaces Routing DHCP and DNS Diagnostics Firewall

8. Zones那里, 点add



Drop invalid packets ☐

Input accept ▾

Output accept ▾

Forward reject ▾

## Routing/NAT Offloading

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading ☐

? Software based offloading for routing/NAT

## Zones

| Zone ⇒ Forwardings        |  | Input    | Output   | Forward  | Masquerading                        |   |             |
|---------------------------|--|----------|----------|----------|-------------------------------------|---|-------------|
| lan ⇒ wan                 |  | accept ▾ | accept ▾ | accept ▾ | <input type="checkbox"/>            | ≡ | Edit Delete |
| wan ⇒ lan                 |  | accept ▾ | accept ▾ | reject ▾ | <input checked="" type="checkbox"/> | ≡ | Edit Delete |
| Add                       |  |          |          |          |                                     |   |             |
| Save & Apply ▾ Save Reset |  |          |          |          |                                     |   |             |

9. 按下图设置, 点save

Firewall - Zone Settings

General Settings

Advanced Settings

Conntrack Settings

This section defines common properties of "this new zone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name

vpn\_fw

Input

drop

Output

accept

Forward

drop

Masquerading

☒

🔔

Enable network address and port translation IPv4 (NAT4 or NAPT4) for outbound traffic on this zone. This is typically enabled on the wan zone.

MSS clamping

☒

Covered networks

vpn:

The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic **originating from this new zone**. *Source zones* match forwarded traffic from other zones **targeted at this new zone**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination* zones:

lan

wan

wan6:

▼

Allow forward from *source* zones:

lan

wan

wan6:

▼

Dismiss

Save

10. 点save 返回firewall 页面后再点save & apply

OpenWRT Page 10

OpenWrt

StatusSystemNetworkLogout

UNSAVED CHANGES: 20

Inputaccept

Outputaccept

Forwardreject

### Routing/NAT Offloading

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading☐

Software based offloading for routing/NAT

### Zones

| Zone ⇒ Forwardings  | Input  | Output | Forward | Masquerading                        |                                  |
|---------------------|--------|--------|---------|-------------------------------------|----------------------------------|
| lan ⇒ wan<br>vpn_fw | accept | accept | accept  | <input type="checkbox"/>            | <div><div></div>EditDelete</div> |
| wan ⇒ lan<br>vpn_fw | accept | accept | reject  | <input checked="" type="checkbox"/> | <div><div></div>EditDelete</div> |
| vpn_fw ⇒ lan<br>wan | drop   | accept | drop    | <input checked="" type="checkbox"/> | <div><div></div>EditDelete</div> |

Add

Save & Apply

Save

Reset

11. 现在, 如果电脑手机连在这个路由器上, 就可以自由上网了