福达 VPN 产品使用手册

公司：福达新创通讯科技（厦门）有限公司

地址：福建省厦门市软件园二期望海路 39 号 416 室

电话：0592-3732988 #8001

传真：0592-3732988

邮箱：sales@vidagrid.com

网址：www.vidagrid.com

声　明

本手册中的内容将来会有所调整，受条件限制，无法另行通知，更改的内容将会在再版时补充至本手册。本公司保留在任何时间做出调整或修正本手册内容（包括手册中描述的产品或程序）的权利。

本公司对本手册的内容不做任何承诺、明示或默许担保。其中包括手册内容的适应性或符合特定使用目的的默许担保，且福达新创不对用户使用该产品侵犯第三方权利或利益负责。

本公司依据中华人民共和国著作权法，享有及保留一切著作之专属权力，未经本公司同意，不得对本手册进行改编、翻印、改造或效仿等。

目录

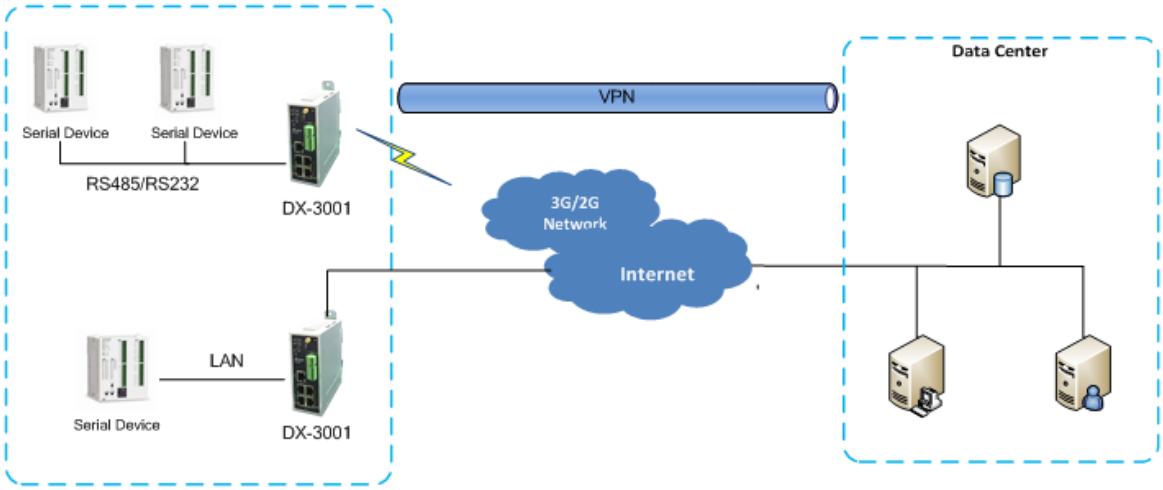
第一章 产品介绍

1.1 产品概览

福达 VPN 工业路由器，基于双 SIM 卡的设计，比如 WCDMA、UMTS, HSUPA, GSM, GPRS, and EDGE。当一张 SIM 卡网络有问题的时候，设备能够自动地切换到另外一个移动网络。除了双 SIM 卡网络外，还支持通过 WAN 口连接有线网络到 Internet。WAN 口和 SIM 卡网络的优先级可以自定义。由于设备只内置了一个 3G 模块，所以两张 SIM 同一时刻只能有一张 SIM 卡起作用。

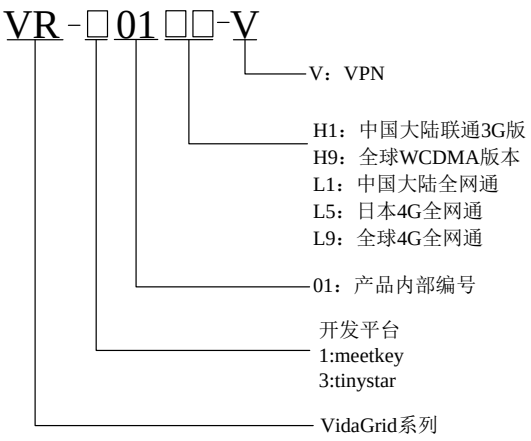
福达 VPN 路由器支持 PPTP、L2TP、OPENVPN 和 GRE 等多种标准的 VPN。其自带丰富的接口包括以太网口，RS232，RS485 以满足多种设备可以被接入进来。

该产品被广泛的适用于 M2M 的领域，比如工业自动化、智能电网、金融、环境监控、楼宇自动化、智能交通、视频监控、自动贩卖机等。



1.2 选型

福达 VPN 路由器命名规则



福达 VPN 路由器选型表

模块 / 功能		VR-100 系列		VR-300 系列		
		VR-101H1-V	VR-101L1-V	VR-301H9-V	VR-301L1-V	VR-301L5-V
联网方式	SIM 卡制式	中国大陆联通 3G	中国大陆 4G 全网通	全球 WCDMA（3G）	中国大陆 4G 全网通	日本 4G 全网通
	有线网接入	支持	支持	支持	支持	支持
	Wifi (Client)	支持	支持	NA	NA	NA
硬件接口	RS232	1◈	1◈	1	1	1
	RS485	1◈	1◈	1	1	1
	以太网口	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN
VPN 功能	IPSec Client	支持(不带证书)	支持(不带证书)	支持	支持	支持
	IPsec Server	NA	NA	支持	支持	支持
	PPTP client	支持(不带证书)	支持(不带证书)	支持	支持	支持
	L2TP client	支持(不带证书)	支持(不带证书)	支持	支持	支持
	Open VPN client	支持(不带证书)	支持(不带证书)	支持	支持	支持
防火墙功能	SPI 防火墙	支持	支持	支持	支持	支持
	DMZ	支持	支持	支持	支持	支持
	端口映射	支持	支持	支持	支持	支持
	端口触发	支持	支持	支持	支持	支持
	NAT 地址转换	支持	支持	NA	NA	NA
	URL 过滤	支持	支持	支持	支持	支持
	IP 过滤	支持	支持	支持	支持	支持
	MAC 过滤	支持	支持	支持	支持	支持
协议	MODBUS TCP	NA	NA	网口	网口	网口
	MODBUS RTU	NA	NA	RS232/RS485	RS232/RS485	RS232/RS485
	MODBUS ASCII	NA	NA	RS232/RS485	RS232/RS485	RS232/RS485
	SNMP	NA	NA	网口	网口	网口

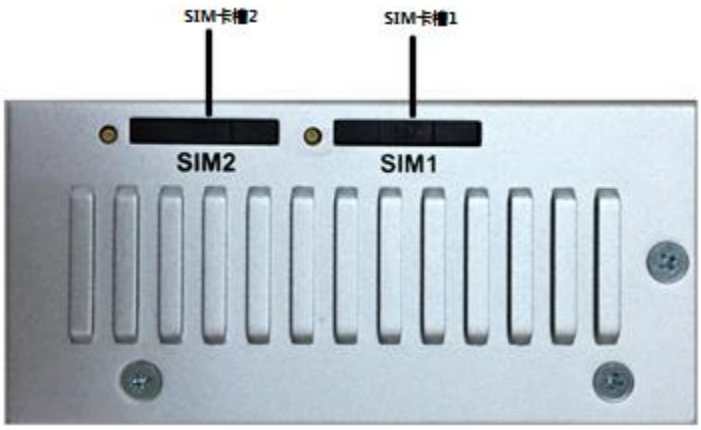
Ps：（1）◈作为硬件预留接口，没有对应功能

1.3 外观及其安装尺寸

福达 VPN 路由器的尺寸均是同一个，包含双 SIM 卡。

1.3.1 正面面板及其指示灯

1.3.2 顶部平面



1.3.3 底部平面

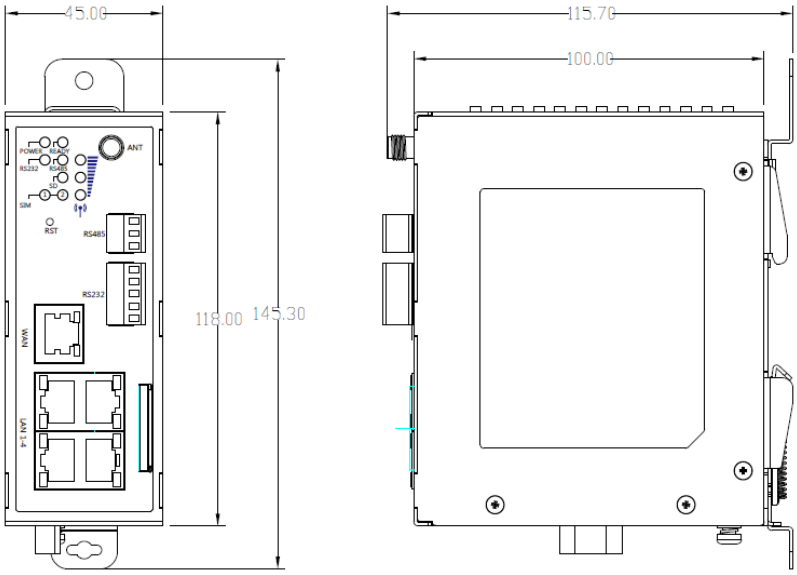
注：

复位按钮位于路由器的正面。通过按复位按钮可以实现重启路由或回复出厂的介绍。具体的定义如下：

- 在设备正常运行的状态下，短按是重启路由，长按（3~6S）是恢复出厂设置。
- 恢复出厂设置的时候，RST 按钮被按下到达恢复出厂条件的时候所有指示灯除 Power 指示灯之外，会全闪一下。

1.3.4 安装尺寸

单位 ： mm



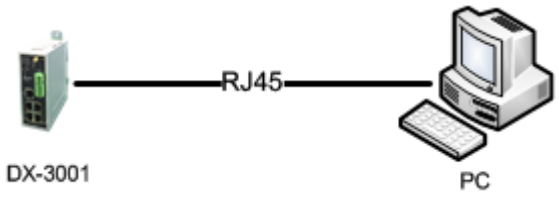
第二章 WEB 配置页面访问

DX-3001 是一款工业级以太网 VPN 路由器，内置友好的 WEB 配置页面。客户可以通过 WEB 快速配置 VPN 路由器。

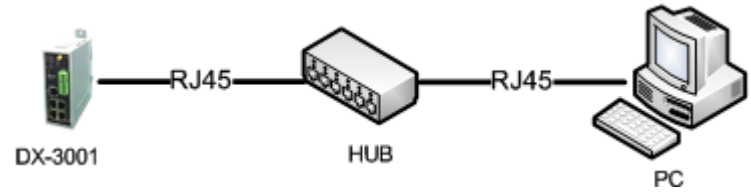
2.1 连线

用一根 RJ45 的网线或交换机将电脑和 PC 连接起来。

（1）网线直连



（2）通过 HUB 或者 Switch 配置。



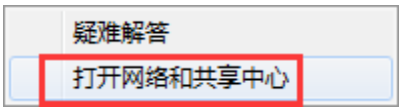
2.2 默认 IP 和登陆账号及密码

默认 IP 地址是 192.168.1.1。 默认的用户名和密码：admin/admin。

2.3 更改电脑 IP

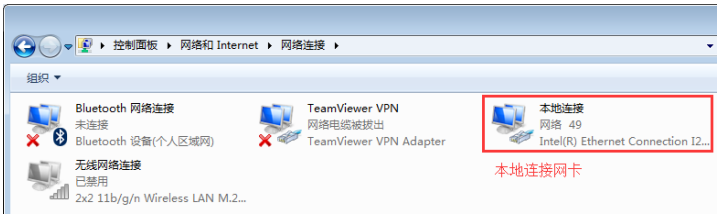
找到电脑右下角的网络图标。

右键下角的网络图标，出现，



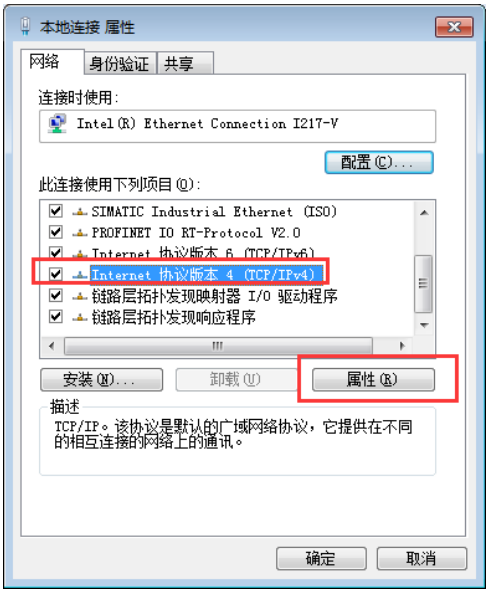
点击【打开网络和共享中心】

点击【更改适配器设置】

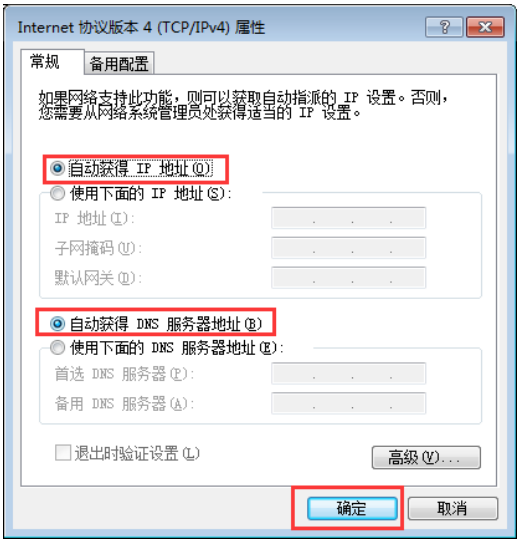


右键“本地连接”

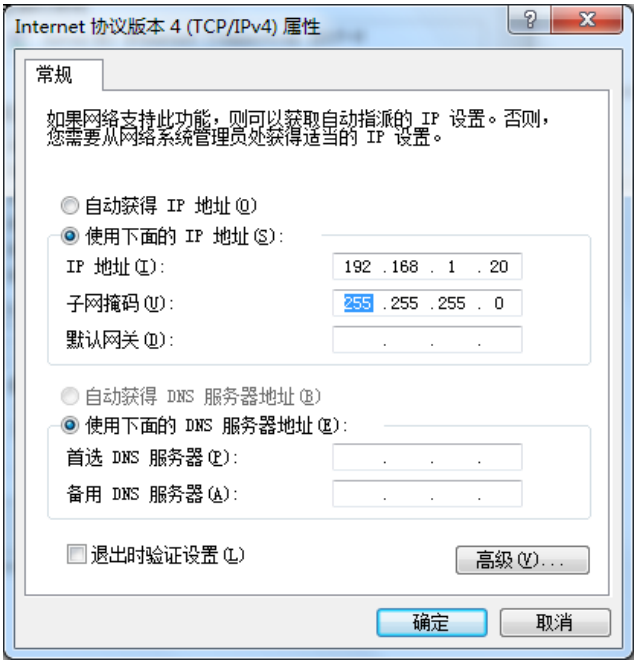
点击【属性】



选中“Internet 协议版本 4（TCP/IP V4）”，点击【属性】



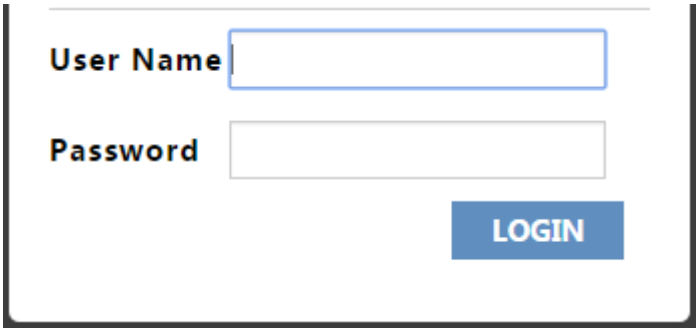
修改为手动，修改后 IP 如下：



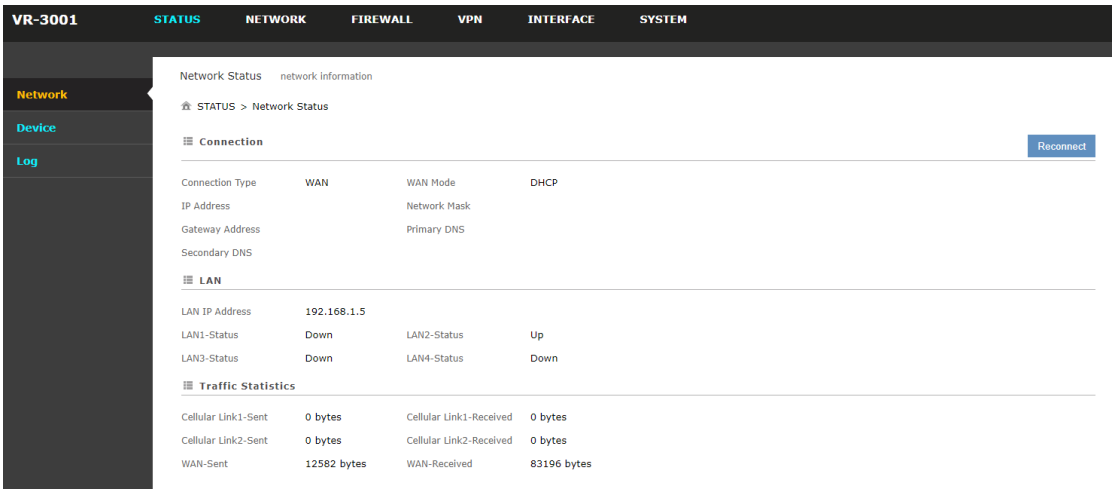
2.4 登陆

1. 打开浏览器的地址栏中输入路由器的 IP 地址（默认 IP 地址 192.168.1.1）

2. 如果 IP 正确的话，将会返回登录画面。输入登录用户名和密码（用户名：admin，密码：admin）



3. 登录后将会显示状态画面下的网络连接状态



注：

为了安全起见，您在登录后最好立即修改登录的密码。

第三章 功能说明

3.1 状态

显示一些设备的概要和详细信息，比如网络状态、设备信息、日志等。

3.1.1 网络状态

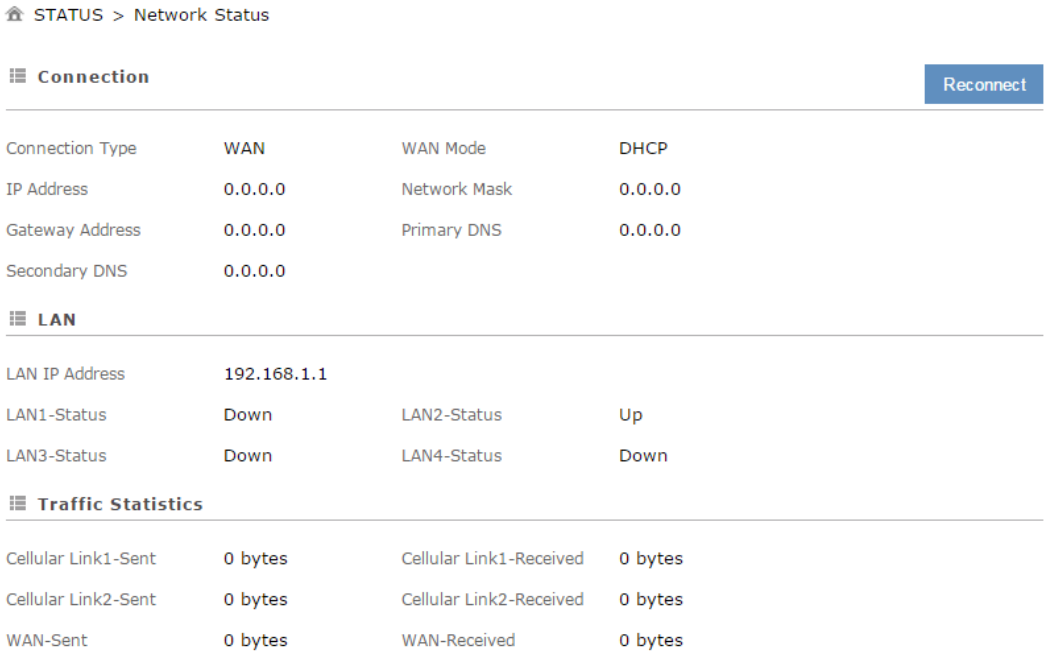
该页面显示基本的网络状态、LAN 口状态和流量等信息。

当连接到 Internet 是通过 WAN 口连接的时候，WAN 口的连接模式，IP 地址，网关，DNS 等信息。（如果没有连接到网络的话，IP 等信息均为 0.0.0.0）

当连接到 Internet 的时候是通过 SIM 卡网络的时候，将会显示 SIM 卡的信号强度，拨号状态、认证方式、APN 设置、IP 地址等信息。

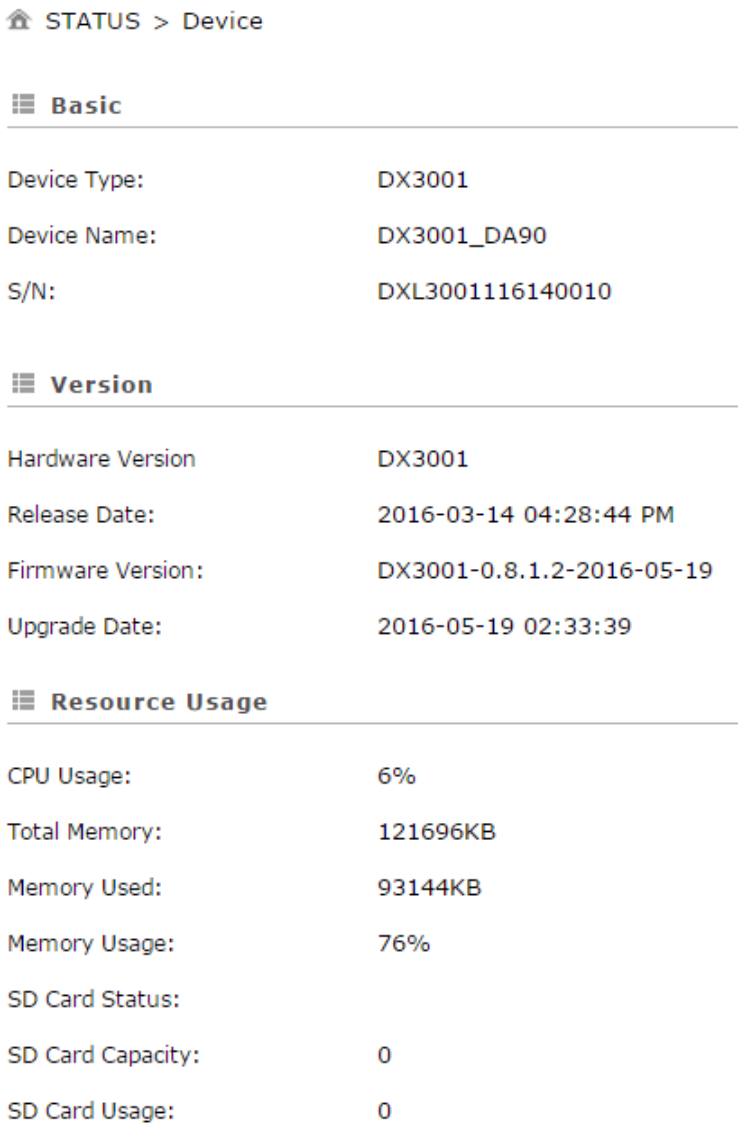
LAN 口的信息包括 IP 地址，以及四个 LAN 的连接状态。（UP 表示有连设备，Down 表示没有连设备）。

流量统计：显示各个接口的流量信息。



3.1.2 设备信息

在这页面中展示了软件和硬件的版本号，和一些存储、CPU 的使用信息。



- 基本

条目	描述
Device Type	路由器的型号
Device Name	路由器的名称。 默认的命名规则： VR301 + “_” + “MAC 地址的后四位”
S/N	路由器的序列号

- 版本

条目	描述
Hardware Version	当前路由器的硬件版本号
Release Date	硬件版本的发布日期
Current Version	当前路由器的韧体版本号

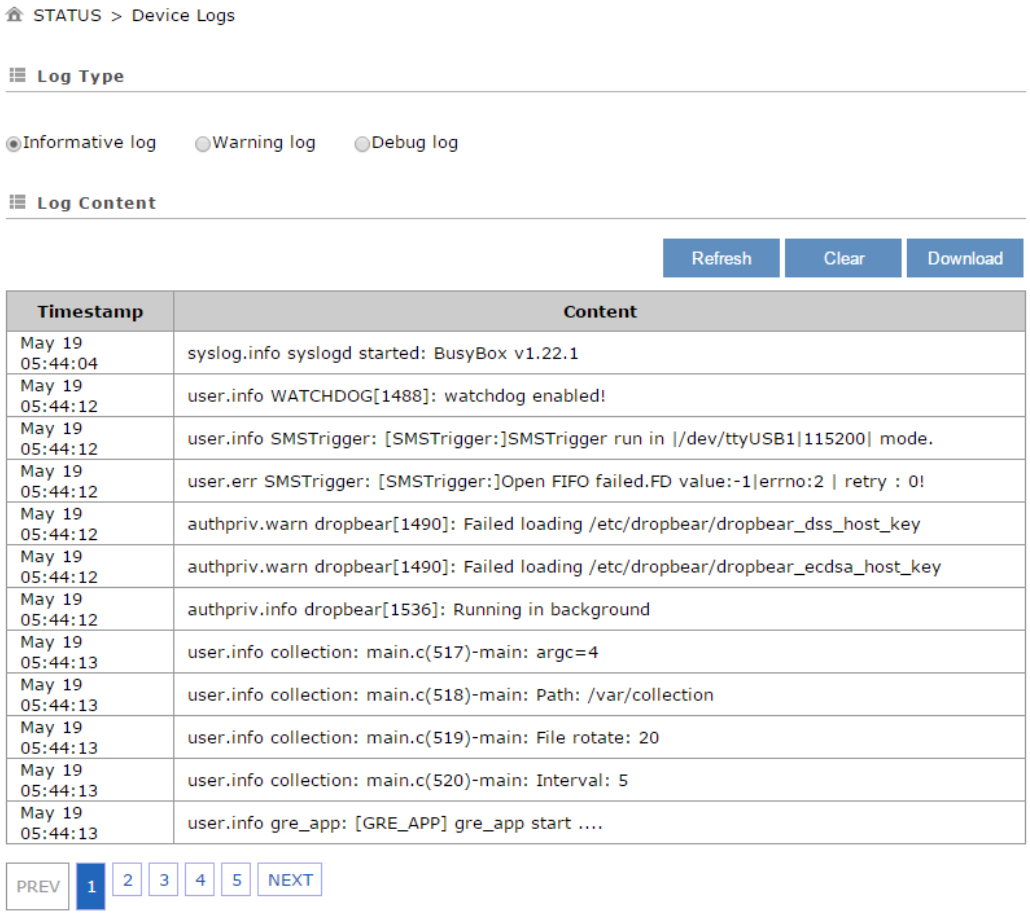
Upgrade Date	路由器最近更新的版本日期

- 硬件资源的使用情况

条目	描述
CPU Usage	当前 CPU 的使用率
Total Memory	总的存储容量
Memory Used	已使用的存储
Memory Usage	当前存储使用占比
SD Card Status	插入路由器的 SD 卡状态
SD Card Capacity	SD 卡中存储容量
SD Card Usage	SD 卡中存储的使用率

3.1.3 日志

日志页面记录路由器的一些重要运行记录。包括系统日志，错误日志，调试日志。可以通过刷新按钮刷新得到当前最新的日志，也可以清除或者下载。



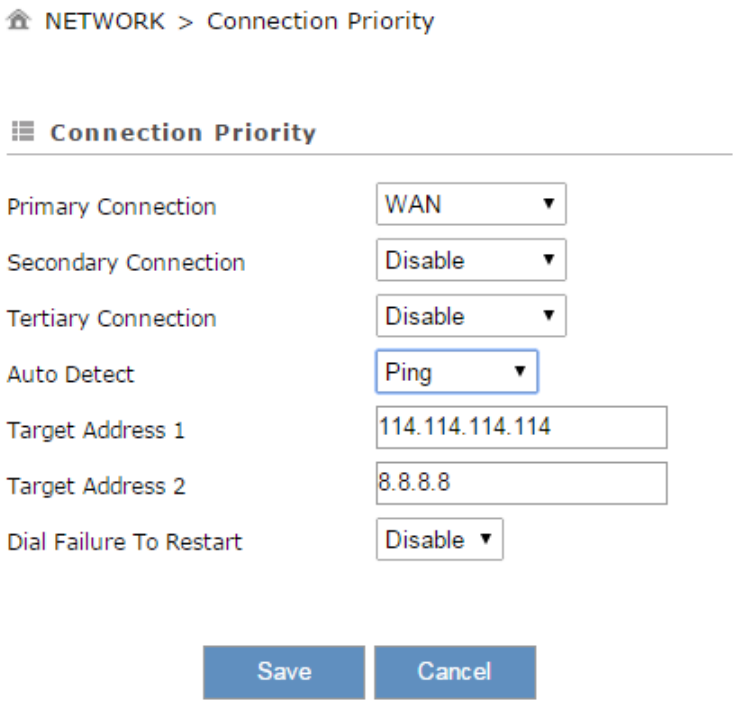
3.2 网络设置

网络设置，可以试着联网的优先级，配置 WAN 口/LAN 口/SIM 卡的设置。

3.2.1 连接优先级配置

可以选择通过那个接口连接到 Internet，并且还可指定优先级。还可以配置自动切换的优先级。

This page is used for setting up the connection priority. Router provide 3 links to connect to Internet, include cellular network 1&2 and WAN, user can appoint the connect order in this page.



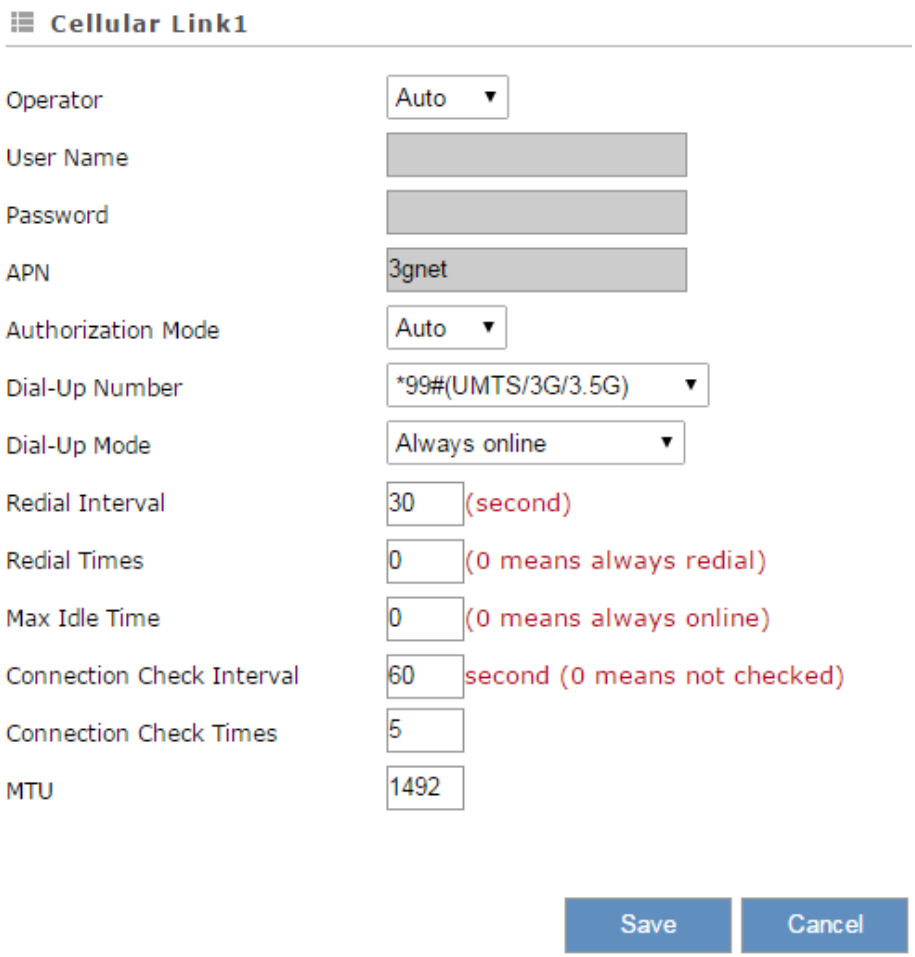
描述	默认设置
Primary Connection	
优先级最高的连接类型	WAN
Secondary Connection	
优先级第二的连接类型	Disabled
Tertiary Connection	
优先级第三的连接类型.	Disabled
Auto Detect	
检测网联网信号的机制。该机制是作为切换的网络的标准。	Disabled
Target Address 1	

描述	默认设置
联网信号检测主要网址	N/A
Target Address 1	
联网检测信号的备用网址	N/A
Dial Failure To Restart	
如果拨号失败，可以进行设置重试多少次没有成功后可以进行重启等动作	Disabled

3.2.2 SIM 卡 1 设置

主要设置 SIM 卡 1 的拨号设置。包括，操作方式，APN，用户名和密码等信息。

NETWORK > Cellular Link1



描述	出厂默认
Operator	
可以通过下拉选框选择自动或者其他模式	AUTO

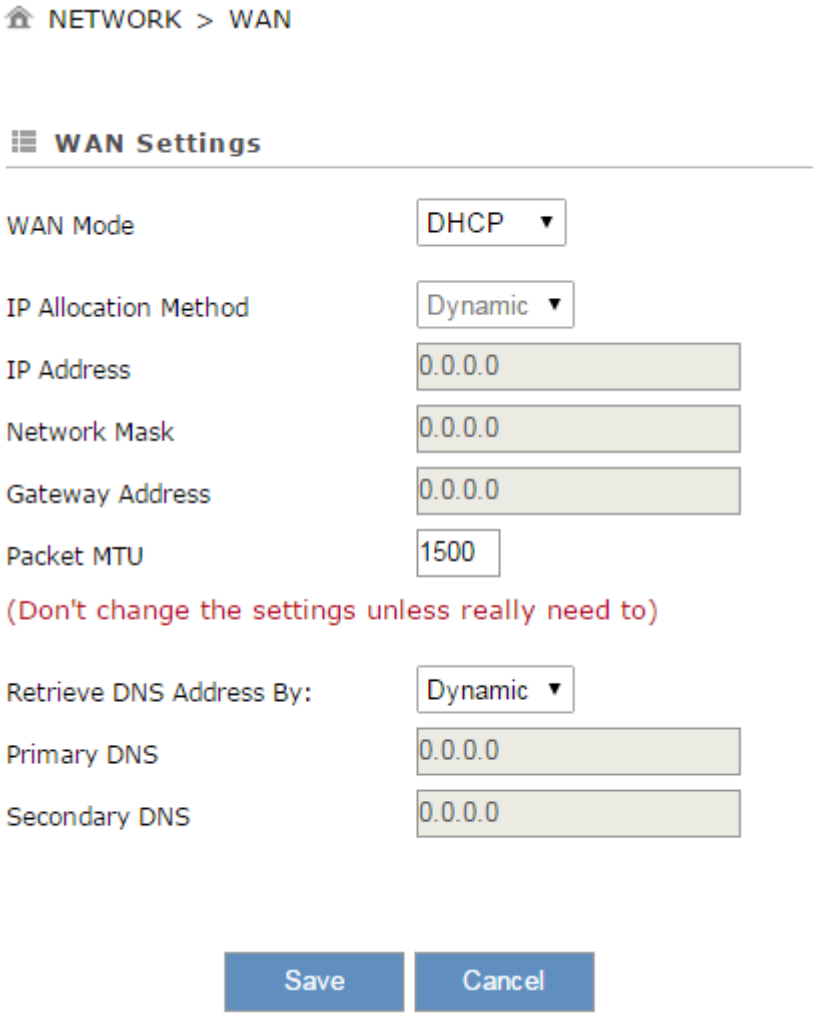
描述	出厂默认
● **Auto:**自动模式下，路由器会去自动检测 SIM 卡的 APN 等设置信息。 ● **Others**: 用户自己手动输入 SIM 卡联网相关纤细	
User Name	
只有在“Other”模式下才能使用。这是运营商在通过 APN 接入的时候需要用户名等参数	N/A
Password	
只有在“Other”模式下才能使用。这是运营商在通过 APN 接入的时候需要密码等参数	N/A
APN (Access Point Name)	
只有在“Other”模式下才能使用。这是 SIM 卡的运营商指定的 APN。详细请咨询相关运营商	3gnet
Authorization Mod	
通过下拉选框可以选择 “Auto”, “PAP” 和“CHAP”等模式。	Auto
Dial-Up Number	
只有在“Other”模式下才能使用。改号码由移动运营商提供	*99#
Dial-Up Mode	
可以操作的选项有 ： ● **Always online**: 保存设备永久在线。在设备拨号不成功的时候，进行重拨。 ● **On-demand connection**:有需要连接到Internet的请求才进行拨号。（但是拨号容易失败，建议慎用） ● **Manual connection**: 如果断开后，需要手动连接	Always online
Redial Interval	
设置当拨号失败后距离下一次拨号的时间间隔，当拨号方式为“始终在线”或“按需连接”时此选项才起作用	30
Redial Times	
设置当拨号失败后尝试重拨最大次数，0 表示无限次重拨，当拨号方式为“始终在线”或“按需连接”时此选项才起作用。	5
Max Idle Time	
设置拨号连接最大空闲时间，当连接空闲时间超过该数值时，路由器将自动断开拨号连接，0 表示不自动断开	180
Connection Check Interval	
设置拨号连接状态检测时间间隔，即检测拨号连接是否断开，若断开则启动重拨进程，0 表示禁用检测功能。	60

描述	出厂默认
Connection Check Times	
设置当检测到拨号连接失败后的最大重拨次数，0 表示无限次重拨	5
MTU	
设置拨号连接最大传输单元，默认值为 1492	1492

3.2.3 SIM 卡 2 设置

参考 SIM 卡 1 的设置。参考上一节。

3.2.4 WAN 设置

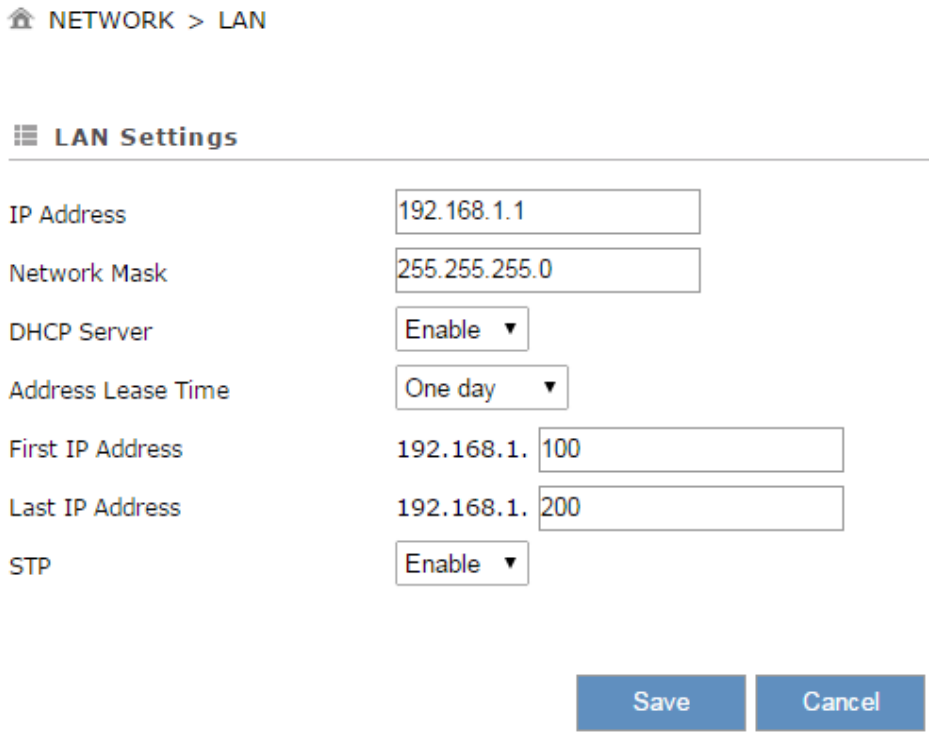


Description	Default
WAN Mode	

Description	Default
WAN 口的接入方式 设置广域网接入方式，可选项为“动态 IP 地址”和“静态 IP 地址” ● 静态 IP 地址:可手动自定义 IP 地址. ● 动态 IP 地址:IP 地址会经由 动态主机设定协议 (DHCP) 指派 IP 地址给路由器	DHCP
IP Allocation Method	
根据接入方式自动匹配： ● 动态获取: 从 DHCP 服务器动态获取 IP 地址、掩码、网关等相关信息. ● 手动指定: 手动指定 IP 地址、掩码、网关等相关信息	DHCP
IP Address	
设置路由器接入广域网的 IP 地址	0.0.0.0
Network Mask	
设置路由器 LAN 口子网掩码	0.0.0.0
Gateway Address	
设置路由器接入广域网的网关地址	0.0.0.0
MTU	
设置数据包最大传输单元	1500
Retrieve DNS Address By	
接入方式选择“动态 IP 地址”，获取 DNS 的方式可以是“动态获取”或者“手动指定”； 接入方式选择“静态 IP 地址”，获取 DNS 的方式可以只能选择“手动指定”	DHCP
Primary DNS	
设置路由器接入广域网的主域名服务器 IP 地址	0.0.0.0
Secondary DNS	
设置路由器接入广域网的从域名服务器 IP 地址	0.0.0.0

3.2.5 LAN 设置

本页主要是对 LAN（局域网）进行设置，包括配置 IP 地址、子网掩码、DHCP 服务器等信息。



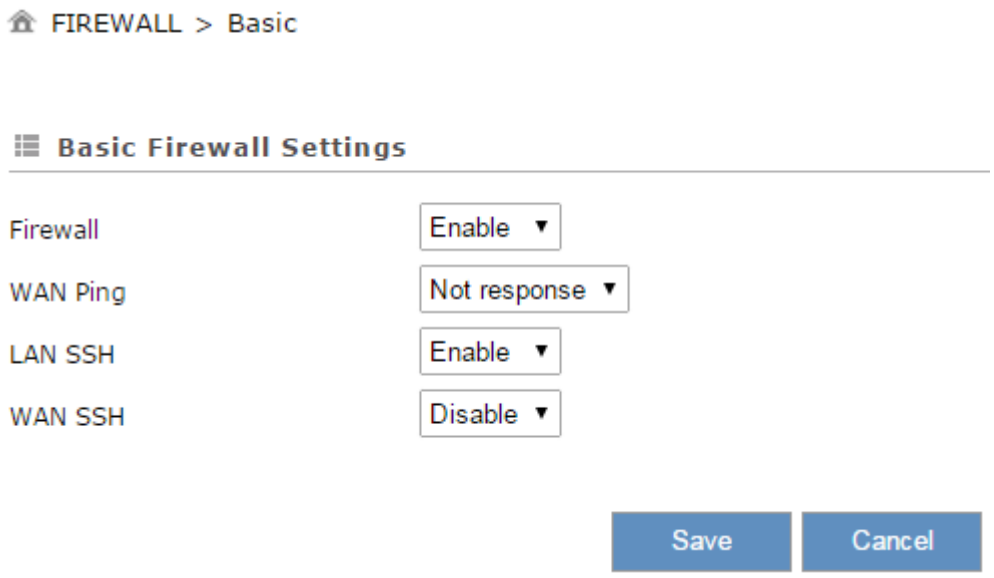
描述	默认值
IP Address	
设置路由器 LAN 口 IP 地址	192.168.1.1
Network Mask	
设置路由器 LAN 口子网掩码	255.255.255.0
DHCP Server	
DHCP 服务器功能开关，取值为“启用”“禁用”	Enable
Address Lease Time	
设置 DHCP 服务器所分配的 IP 地址的租用时间，取值为“一天”、“两天”、“三天” 。	One day
First IP Address	
设置 DHCP 服务器地址池起始地址	192.168.1.100
Last IP Address	
设置 DHCP 服务器地址池结束地址	192.168.1.200
STP	
STP 的作用是通过阻断冗余链路，使一个有回路的桥接网络修剪成一个无回路的树形拓扑结构，防止报文在环路网络中的增生和无限循环。开启该功能会增加流量消耗。	Enable

3.3 防火墙设置

防火墙设置包括基本设置、DMZ 设置、端口映射、端口触发、URL 过滤、MAC 过滤、IP 地址过滤等七个子配置页面。

3.3.1 Basic（防火墙基本设置）

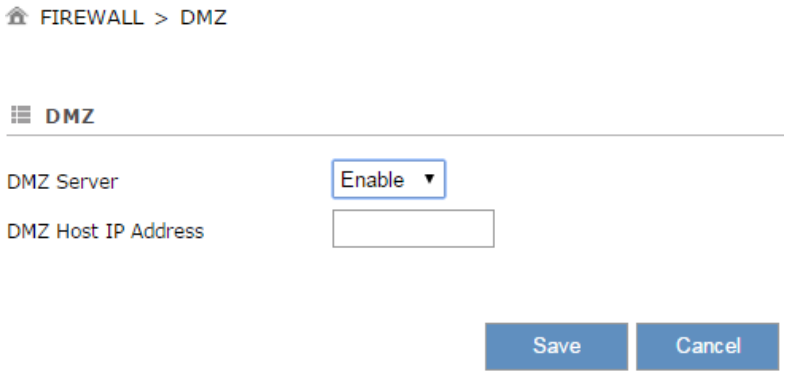
本页主要配置基本防火墙设置，包括 SPI 防火墙开关、外网 Ping 响应、LAN SSH 功能及 WAN SSH 功能。



描述	默认值
Firewall	
防火墙功能开关，可选值“启用”“停用”。 开启后可以防止 DDOS 等攻击。	Enable
WAN Ping	
设置是否响应由外网发来的 Ping 命令，可选值“响应”“不响应”。	Not responded
LAN SSH	
设置是否允许 LAN 端通过 SSH 连接路由器，可选值“启用”“停用”。	Enable
WAN SSH	
设置是否允许 WAN 端通过 SSH 连接路由器，可选值“启用”“停用”	Disable

3.3.2 DMZ 设置

本页主要配置 DMZ 服务器。



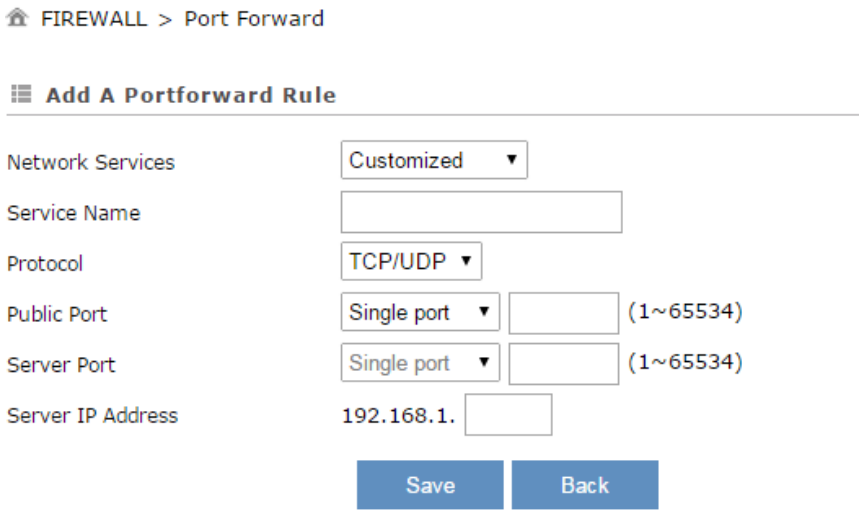
描述	默认值
DMZ Server	
DMZ 服务器开关，可选项“启用”“停用”。	Disable
DMZ Host IP Address	
设置 DMZ 主机 IP 地址。	N/A

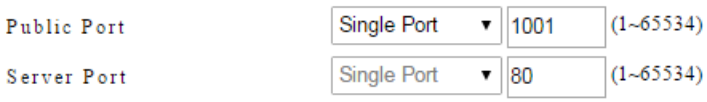
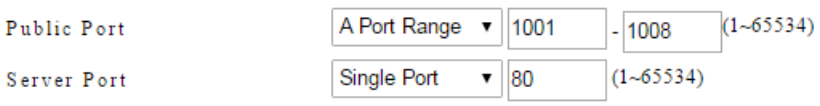
3.3.3 Port Forward 设置

本页主要用于设置端口映射，包括配置服务名、协议、端口、服务器 IP 地址等。通过 “添加映射”按钮用户可向路由器中添加端口映射条目。

点击“Add A Portforward Rule”可以增加一条端口映射的规则

点击“Add A Portforward Rule”后将看到如下页面。



Description	Default
Network Services	
选择常用网络服务，可选值请参照下面常用服务列表	Customized
Service Name	
设置端口映射服务名称，名称由字母、数字，下划线组成，以字母或数字开头，字符串最大长度为 32 个字节。	N/A
Protocol	
选择端口映射协议类型，可选值“TCP/UDP”，“TCP”，“UDP”。	TCP/UDP
Public Port	
设置外部主机（即路由器）端口，可指定“单一端口”或“端口范围”；选择指定端口范围时，端口范围为 1~65534，起始端口必须小于等于结束端口。（注意，别使用常规已经定义的端口，否则会引起异常）	Single Port
Server Port	
设置内部映射端口： 1. 当外部端口选择“单一端口”模式，映射端口只能选择“单一端口” 2. 当外部端口选择“端口范围”模式，映射端口可选择“单一端口”或者“端口范围”。 3. 选择“单一端口”，则外部所由端口范围都映射到单一端口上。 4. 选择“端口范围”，则端口范围和外部端口范围一致，并一一对应映射。 不同端口映射设置结果示例： 1:1 模式  N:1 模式  N:N  	Single Port
Server IP Addres	
设置应用该端口映射规则的服务器 IP 地址。	192.168.1.*

端口映射常用服务列表

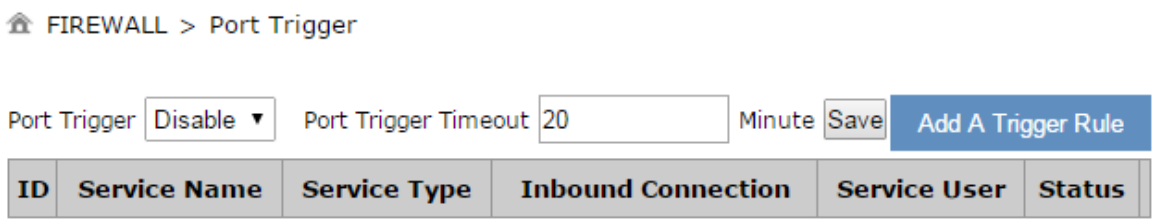
服务名	协议	起始端口	结束端口
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	TCP	20	21
HTTP	TCP	80	80
ICUII	TCP	23566	23566
IP_PHONE	TCP	6670	6670
NetMeeting	TCP	1720	1720
News	TCP	119	119
PPTP	TCP/UDP	1723	1723
Telnet	TCP	23	23
QuakeII/III	TCP/UDP	27960	27960
Real-Audio	TCP	6970	7170

3.3.4 Port Trigger 设置

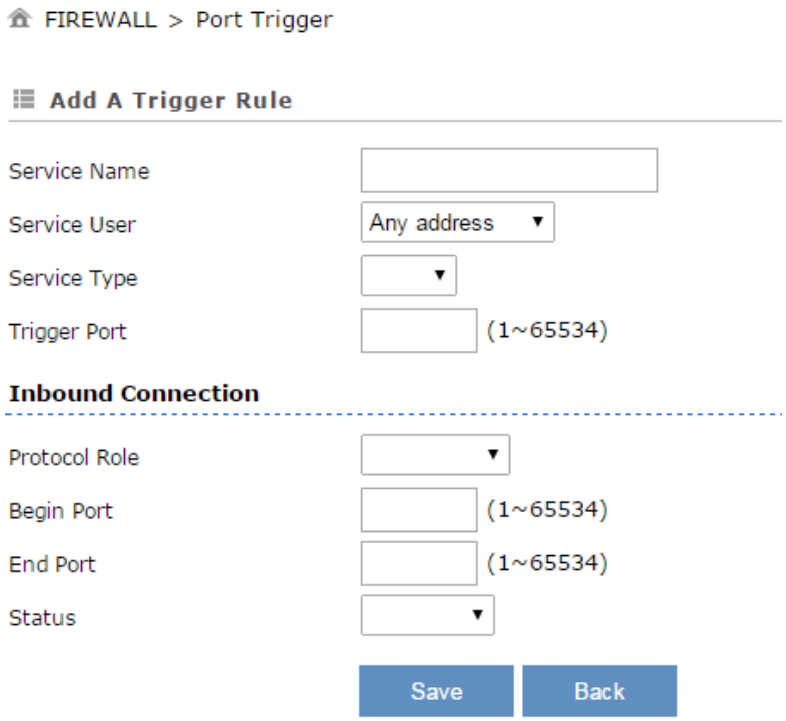
本页主要用于设置端口触发 ,包括配置服务名 、服务用户 、服务类型 ,触发端口等 ,通过 “ADD A Trigger”按钮用户可向路由器中添加端口触发条目 。

端口触发是一种通过一个触发端口来启用或停用一条端口映射规则。当有数据到达触发端口，则映射关系会被打开。

点击按钮 “Add ATrigger Rule” 可以增加一条端口触发的规则。



点击 “Add A Trigger Rule” 按钮后，将会切换到如下画面。

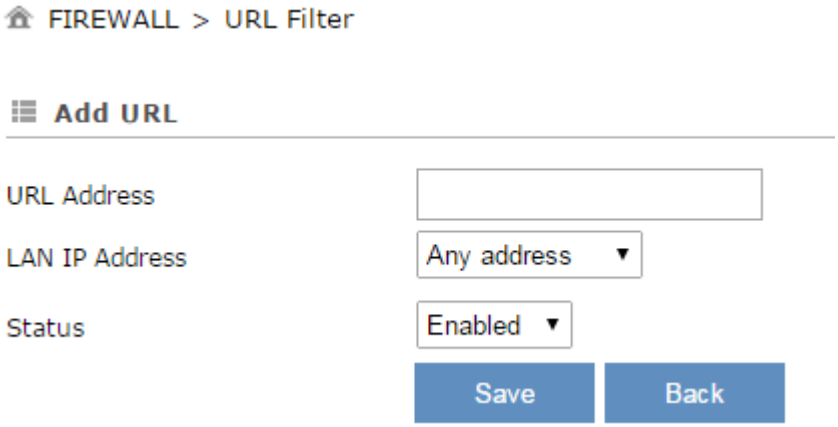


描述	默认值
Service Name	
设置端口触发的名称。名称只能是字母、数字或者下划线的组合，最的长度不能超过 32 个字符。	N/A
Service User	
选择端口触发规则服务用户，可选值“单一地址”“任何”。	Any Address
Service Type	
选择输入连接类型，可选值“TCP/UDP”，“TCP”，“UDP”。	TCP
Triggering Port	
设置触发端口，端口范围 1~65534.	N/A
Protocol Role	
Set up the protocol type for the inbound connection.	TCP/UDP
Begin port	
设置端口触发输入连接起始端口，端口范围 1~65534.	N/A
End Port	
设置输入连接结束端口，端口范围 1~65534.	N/A
Status	
设定该条触发的状态，可选值“失效”“生效”。	Disable

3.3.5 URL 过滤设置

本页主要用于设置 URL 过滤，包括 URL 地址、局域网 IP 地址、状态等。通过 “Add An URL Address”按钮用户可向路由器中添加 URL 过滤条目。

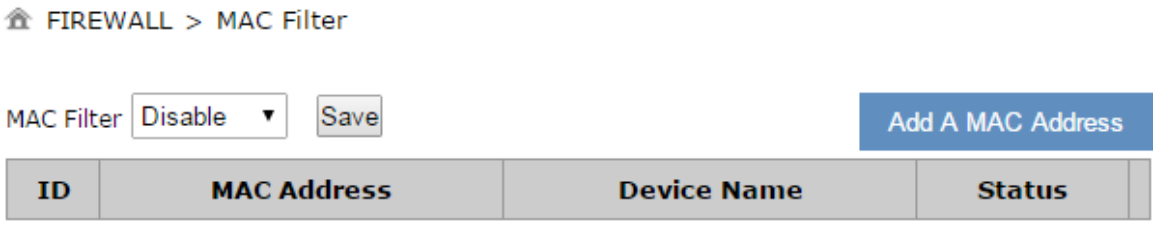
After clicking the “Add An URL Address”, you will see the following page.



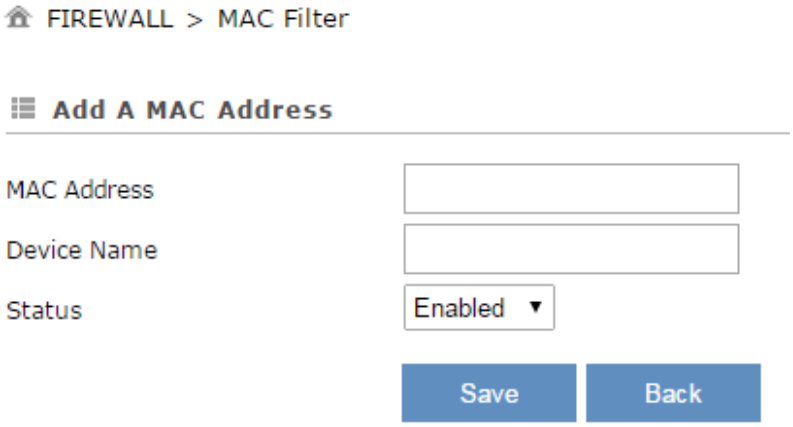
Description	Default
URL Address	
设置所要过滤 URL 地址，如 www.baidu.com。	
LAN IP Address	
设置 URL 过滤所针对的局域网 IP 地址范围，可选项“任何”“单一地址”“地址范围”。	Any Address
Status	
设定该条过滤规则当前状态，可选项“生效”“失效”。	Enable

3.3.6 MAC 地址过滤

本页主要用于设置 MAC 过滤，包括 MAC 地址、设备名称、状态等。通过 “Add A MAC Address”按钮用户可向路由器中添加 MAC 过滤条目。



点击 “Add A MAC Address”按钮后，你将会看到如下的页面。

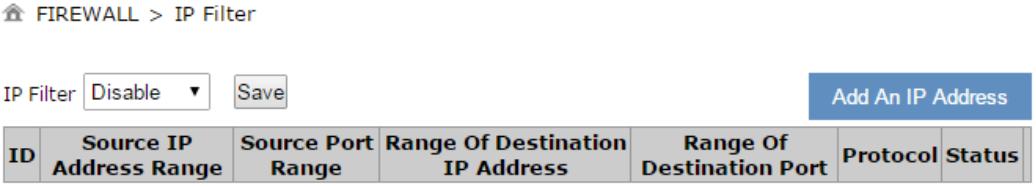


描述	默认值
MAC Address	
设置所要过滤 MAC 地址。	
Device Name	
设置该 MAC 地址对应设备名称。	
Status	
设定该条过滤规则当前状态，可选项“生效”“失效”。	Enable

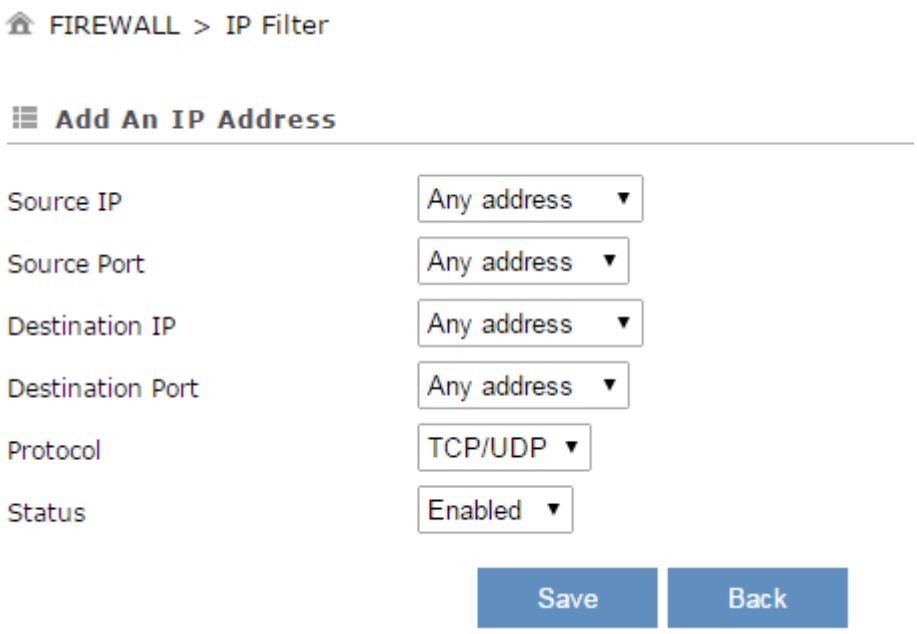
3.3.7 IP 过滤设置

本页主要用于设置 IP 地址过滤，包括源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输协议、状态等。通过 “添加地址”按钮用户可向路由器中添加 IP 地址过滤条目。

IP 过滤是用于过滤某个 IP 地址访问网络的需求。通过选择“Enable/Disable”的选择框来激活这个功能。



点击“Add An IP Address”按钮后看到如下的页面。



Description	Default
Source IP	
设置源 IP 地址，可选项“任何”“单一地址”“地址范围”。	Any Address
Source Port	
设置源端口号，可选项“任何”“单一端口”“端口范围”。	Any Address
Destination IP	
设置目的 IP 地址，可选项“任何”“单一地址”“地址范围”。	Any Address
Destination Port	
设置目的端口号，可选项“任何”“单一端口”“端口范围”。	Any Address
Protocol	
选择地址过滤协议类型，可选值“TCP/UDP”，“TCP”，“UDP”。	TCP/UDP
Status	
设定该条过滤规则当前状态，可选项“生效”“失效”，默认“生效” 。	Enable

3.3.8 IP 过滤设置

主要用于网络地址转换的规则。用户最多可维护 10 条规

NAT 网络地址转换分为原地址转换（SNAT）和目标地址转换（DNAT）

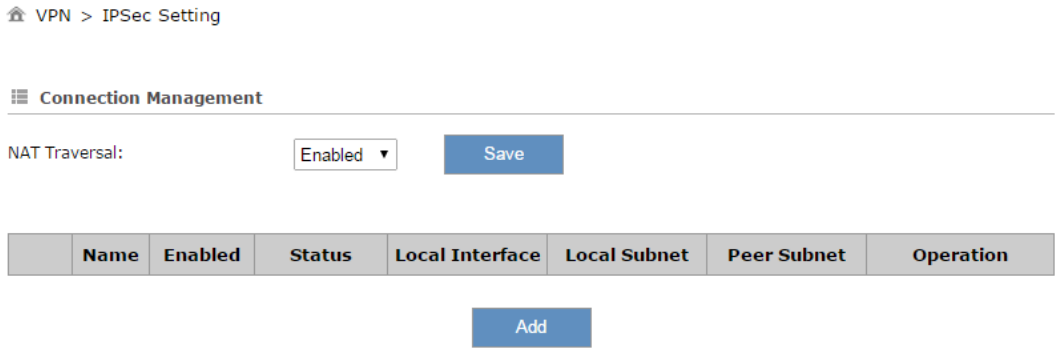
条目	说明
动作	可选项：SNAT/DNAT SNAT：源地址转换，将 IP 数据包的源地址转换成另一个地址。 DNAT：目的地址转换，将本地合法的内部地址，映射到合法的外部地址
源网络	可选项：Inside/Outside Inside：内部地址。Outside：外部地址
转换类型	选择网络地址转换类型，当前只支持 IP to IP
匹配地址	设置要转换的匹配地址
转换地址	设置要转换成的地址
编辑	用于编辑该条规则，打开规则编辑页面
删除	用于删除该条规则

3.4 VPN 设置

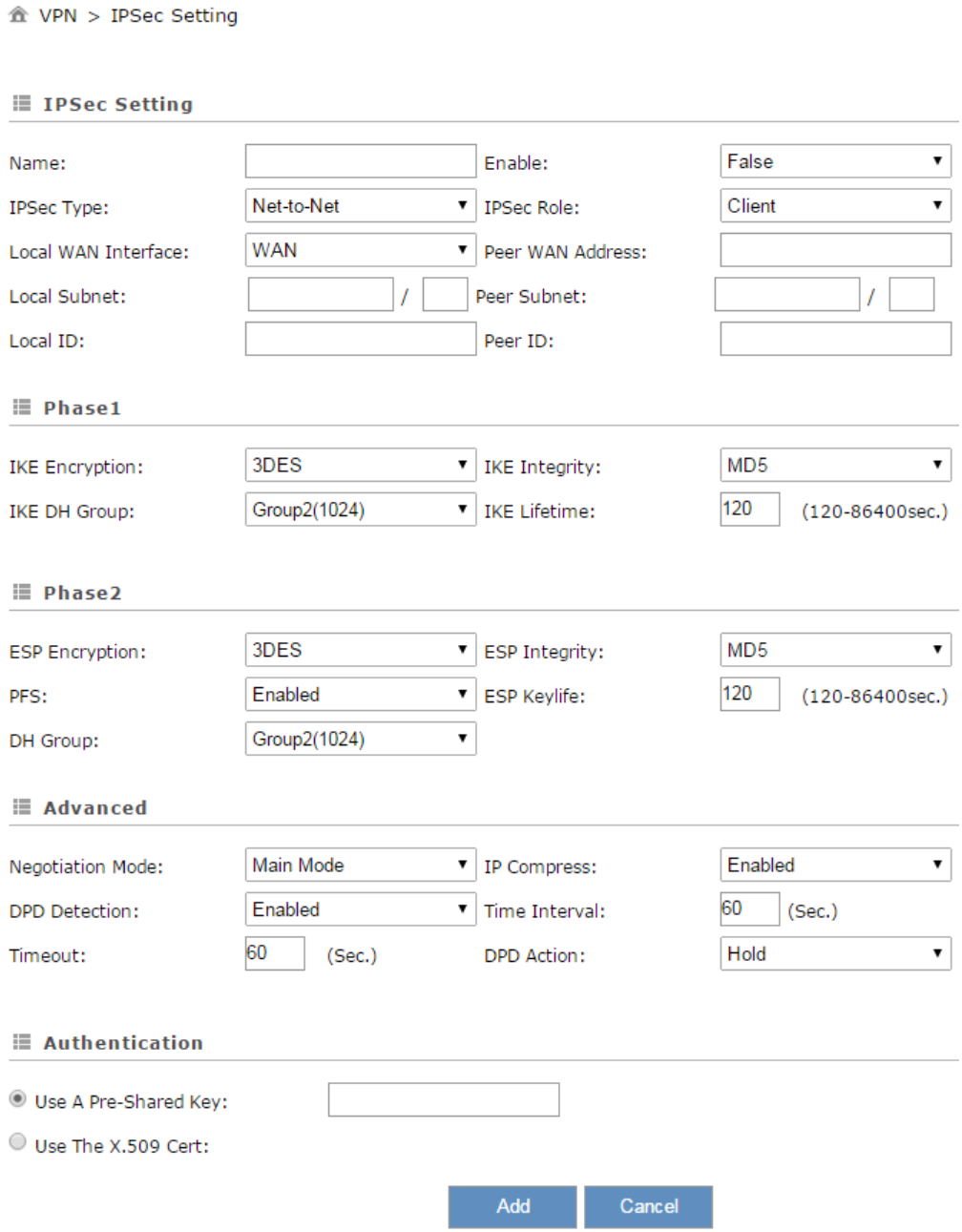
你能够通过这个功能来配置 VPN，其支持 IPsec，OPENVPN，PPTP，L2TP 和 GRE 等标准 VPN。同时对于这些功能还提供证书的导入，VPN 日志的下载。

3.4.1 IPSec 设置

下面这页面用来设置 IPSEC 的 VPN 参数。



点击“ADD”后，



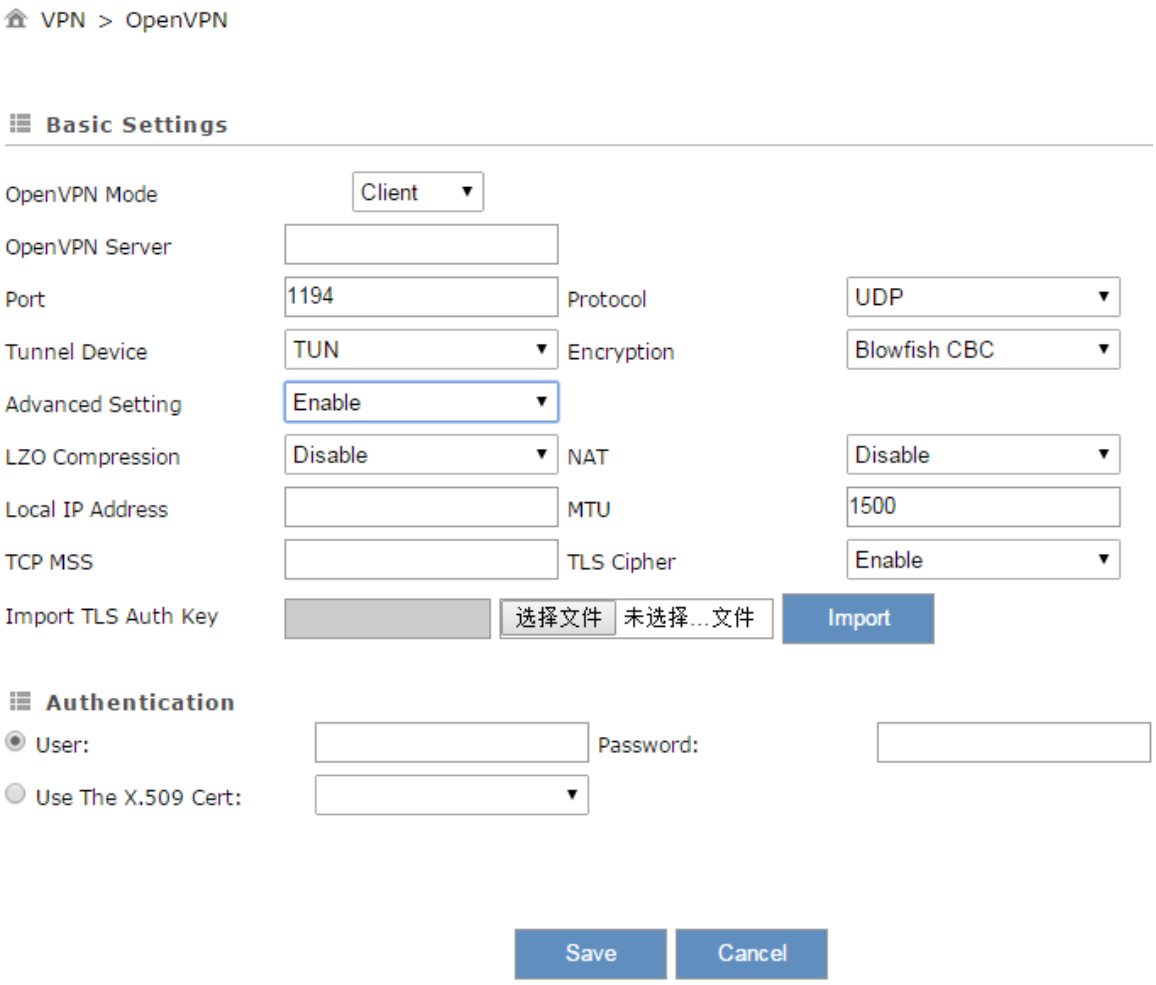
描述	默认值
Name	
输入 IPsec 连接的名称。名称之间不能重复，长度不能超过 20 个字节。	
Enable	
开启和禁用这个连接	False
IPSec Type	
设置 IPSec 的工作模式，目前仅支持 “Net to Net”	Net-to-Net
IPSec Role	

描述	默认值
路由器在 IPsec 连接中的属性，当前支持“Client”和“Server”模式	Client
Local WAN Interface	
本地 WAN 接口设置，目前仅支持设置为 WAN 接口。	WAN
Peer WAN Address	
输入对端的 IP 地址。	
Local Subnet	
输入本地允许进入 IPsec 连接的子网。比如：192.168.1.0/24	
Peer Subnet	
输入对端允许访问的子网。比如 192.168.7.0/24；	
Local ID	
本地节点名称定义	
Peer ID	
对端节点名称的定义	
IKE Encryption	
IKE 阶段的封装模式。有 “3DES”, “DES”, “AES(128bit)” and “AES(256bit)” 加密封装模式。	3DES
IKE Integrity	
IKE 完整性校验阶段。 选项有“MD5”,”SHA1” and “SHA2(256)”	MD5
IKE DH Group	
IKE 的密匙交换算法 选项有“Group1(768)”, “Group2(1024)” , “Group5(1536)”, “Group14(2048) ”, “Group15(3072)”, “Group16(4096)”, “Group17(6144)” and “Group18(8192)”	Group2(1024)
IKE Lifetime	
IKE 策略有效时间。时间范围 120~86400，单位：秒。	120
ESP Encryption	
ESP 封装模式。选项有“3DES”, “DES”, “AES(128bit)” “AES(256bit)”	3DES
ESP Integrity	
ESP 完整性校验。 选项有 “MD5” ”SHA1”	MD5
PFS	
完美前向加密。是指某一密钥泄露不会影响到其他密钥所保护的信息的安全性。	Enabled

描述	默认值
ESP Keylife	
ESP 密匙的有效时间，时间范围 120~86400，单位：秒。	120
DH Group	
ESP 密匙的交换算法. 选项有 “Group1(768)”, “Group2(1024)” , “Group5(1536)”, “Group14(2048) ”, “Group15(3072)”, “Group16(4096)”, “Group17(6144)” 和“Group18(8192)”	Group2(1024)
Negotiation Mode	
设置 IKE 的协商模式。有协商模式和主模式。 ● 主模式：在对身份保护要求较高的场合，应该使用主模式。 ● 野蛮模式：在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度。	Main
IP Compress	
是否启用 IP 的载荷压缩算法。可以节省流量	Enabled
DPD Detection	
DPD（连接检测）。启动 DPD 功能后，当接收端在触发 DPD 的时间间隔内收不到对端的 IPSec 加密报文时， 能够触发 DPD 查询， 主动向对端发送请求报文，对 IKE 对等体是否存在进行检测。	Enabled
Time Interval	
DPD 的检测时间间隔	60
Timeout	
DPD 检测请求的超时时间。	60
DPD Action	
设 DPD 检测到断开时候的动作。	Hold
Authentication	
可以通过 PSK（预共享秘钥）和 Cert（证书）来进行身份认证。PSK 支持最长 24 个字符；证书可以选择已经导入的证书选项。	

3.4.2 OPENVPN 设置

此页面用于配置 OPENVPN 的参数。当前仅支持 OPENVPN 的 Cilent 模式。

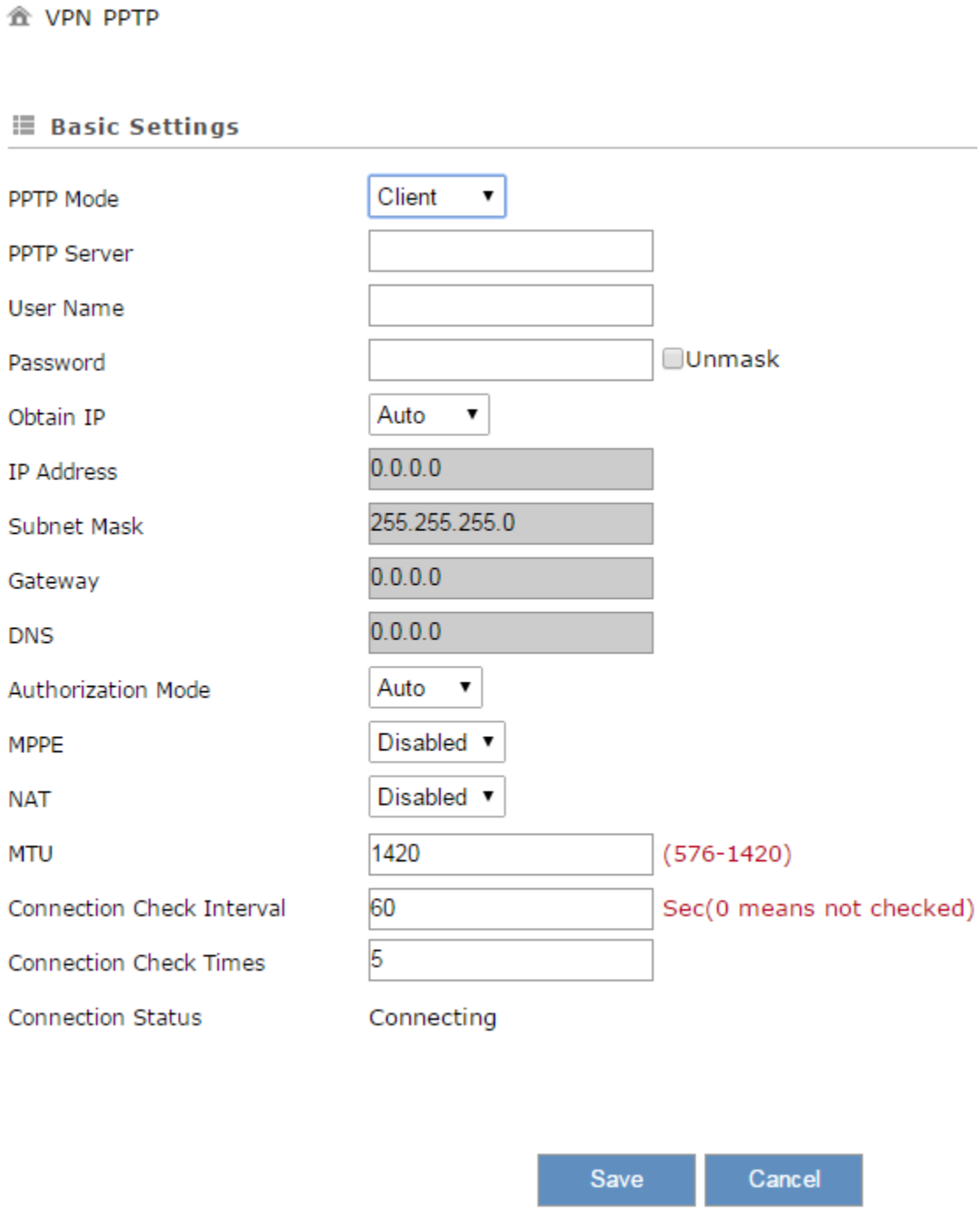


Description	Default
OPENVPN Mode	
启用和禁用 OPENVPN 的 Clinet 功能。	Disabled
OPENVPN Server	
设置 OPENVPN 服务器的 IP 或者域名。	
Port	
设置 OPENVPN 服务器监听的 PORT	1194
Protocol	
设置连接的协议是使用“UDP”还是 TCP “TCP”	UDP
Tunnel Device	
设置接口类型是 “TUN”还是“TAP” TUN –是一个三层设备,也就是说,通过它可以处理来自网络层的数据，更通俗一点的说，通过它，我们可以处理 **IP** 数据包。 TAP –是一个二层设备,也就是说,通过它可以处理来自数据链路层的数据，更通俗一点的说，通过它，来做网卡的桥接。	TUN

Description	Default
Encryption	
选择封装的模式，选项有 “Blowfish CBC”, “AES-128 CBC”, “AES-192 CBC”, “AES-256 CBC” and “AES-512 CBC”	Blowfish CBC
Advanced Setting	
高级设置使能或者禁用。	Disabled
LZO Compression	
启用或者禁用 LZO 压缩	Disabled
NAT	
启用或者禁用 NAT 穿透	Disabled
Local IP Address	
设置本机虚拟的 IP 地址	
MTU	
设置隧道中最大的传输单元长度	1500
TCP MSS	
设置 TCP 数据包每次能够传输的最大数据分段的数据	
TLS Cipher	
设置 TLS(Transport Layer Security) 的封装标准，选项有“AES-128 SHA” and “AES-256 SHA”	Disabled
Import TLS Auth Key	
导入 TLS 认证密匙 Import the authority key of Transport Layer Security	
Authentication	
选择一种认证方式，用户名和密码或者证书认证等选项。	

3.4.3 PPTP 设置

通过这个页面可以设置 PPTP VPN 的参数。当前仅支持 PPTP 客户端模式。

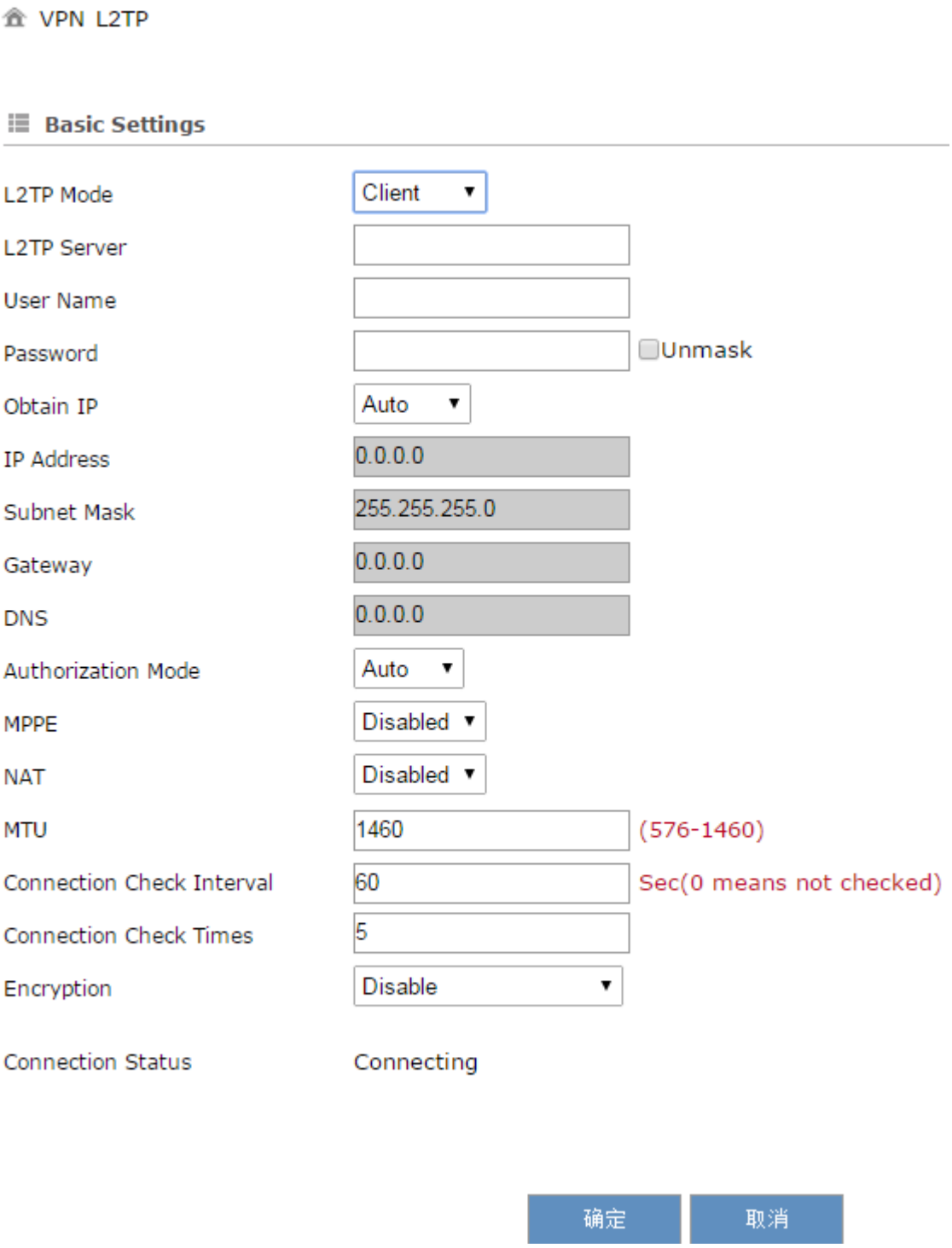


描述	默认值
PPTP Mode	
设置 PPTP 的工作模式，可选择禁用或者 Client 模式	Disabled
PPTP Server	
设置 PPTP 服务器的 IP 或者域名	
User Name	
设置 PPTP 服务器的登陆用户名	

描述	默认值
Password	
设置 PPTP 服务器的登陆密码	
Obtain IP	
设置获取 IP 的方法。可以是自动获取或者手动指定。	Auto
IP Address	
PPTP 客户端的地址	
Subnet Mask	
PPTP 客户端的子网掩码	
Gateway	
PPTP 的客户端的网关	
DNS	
PPTP 客户端的 DNS 服务器地址	
Authorization Mode	
认证方式有 “Auto”, “PAP” 和 “CHAP”.	Auto
MPPE	
启用或禁用微软点到点的封装	Disabled
NAT	
是否启用 NAT（Network Address Translation）功能	Disabled
MTU	
设置隧道中的最大传输单元	1420
Connection Check Interval	
连线检测时间间隔。如果检测到连接失效，将会重连。0 表示不启用该功能。	60
Connection Check Times	
设置检测的次数。当连续检测失败到达指定次数后重启连接。0 代表不启用断线检测功能。	5
Connection Status	
展示当前的连接状态	

3.4.4 L2TP 设置

这个页面可以用来设置 L2TP VPN 参数。当前系统仅支持 L2TP 客户端模式。



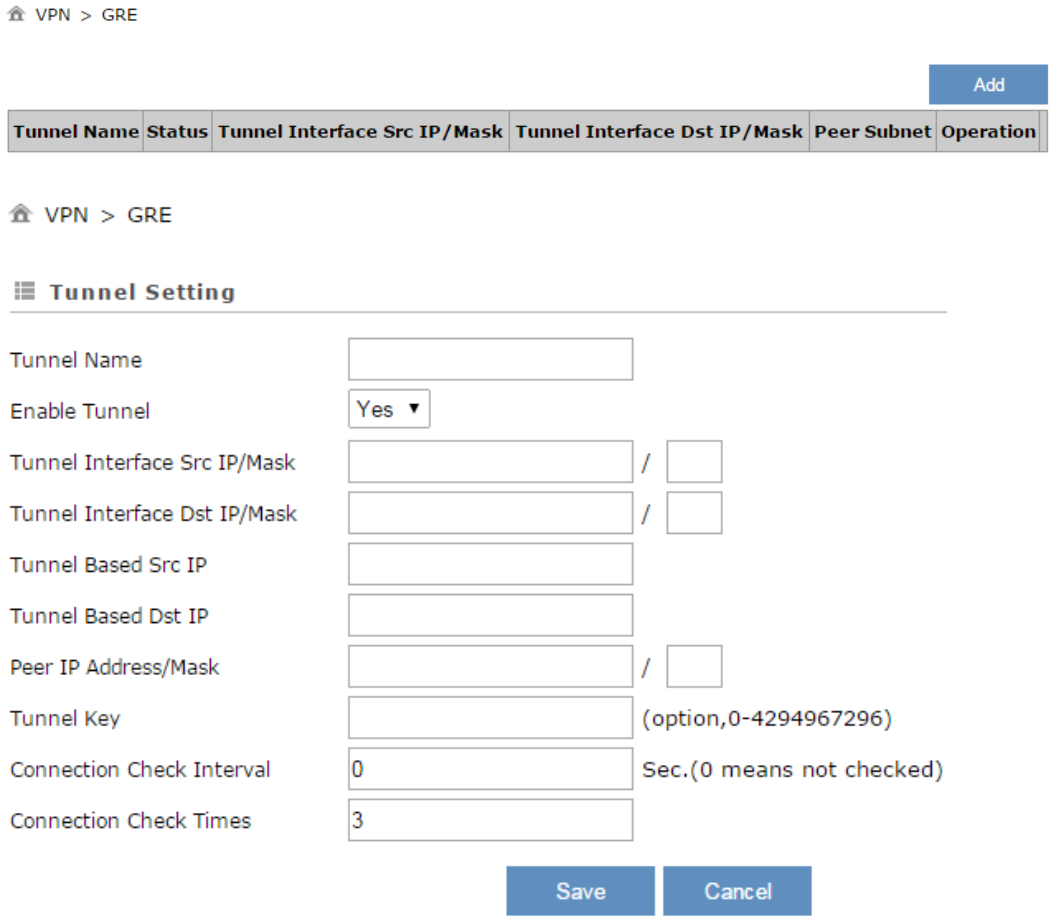
Description	Default
L2TP Mode	
L2TP 模式设置，可以是启用或者禁用。	Disabled
L2TP Server	
设置 L2TP 服务器的域名或者 IP 地址。	
User Name	

Description	Default
设置 L2TP 服务器登陆的用户名	
Password	
设置 L2TP 服务器登陆的命名	
Obtain IP	
设置获取 IP 的方法。可以是自动获取或者手动指定。	Auto
IP Address	
PPTP 客户端的地址	
Subnet Mask	
PPTP 客户端的子网掩码	
Gateway	
PPTP 的客户端的网关	
DNS	
PPTP 的客户端的网关的 DNS 地址	
Authorization Mode	
认证方式有 “Auto”, “PAP” 和 “CHAP”.	Auto
MPPE	
是否启用或者禁用 MPPE（Microsoft Point-to-Point Encryption）功能	Disabled
NAT	
是否启用 NAT（Network Address Translation）功能	Disabled
MTU	
设置隧道中的最大传输单元	1460
Connection Check Interval	
连线检测时间间隔。如果检测到连接失效，将会重连。0 表示不启用该功能。	60
Connection Check Times	
设置检测的次数。当连续检测失败到达指定次数后重启连接。0 代表不启用断线检测功能。	5
Encryption	
设置 L2TP 的封装方式。选项有 “Disabled”, “Use a Pre-Shared Key” 或者 “Use the Certificate”.	Disabled
Input The PSK	
输入 PSK 秘钥	

Description	Default
Select The Certificate	
通过证书功能选择一个证书	
IPSec Peer ID	
输入队短 IPsec 的 ID	
Connection Status	
显示当前 VPN 的连接状态	

3.4.5 GRE 设置

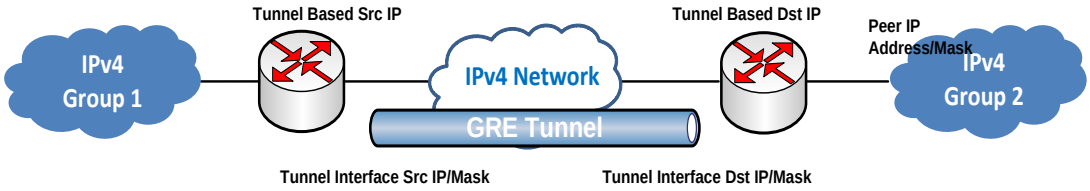
可以通过下面这个页面来设置 GRE VPN 的参数。用户最多创建十条 GRE 隧道。



描述	默认值
Tunnel Name	
输入隧道的名称，隧道间的名称不能重复。	
Enable Tunnel	

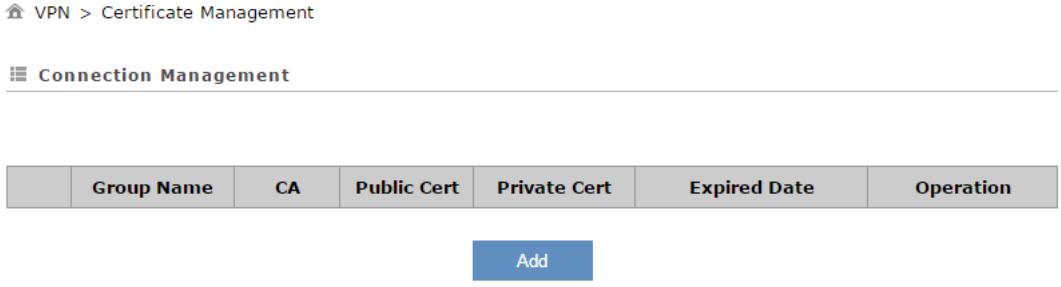
描述	默认值
启用或者关闭当前隧道	Yes
Tunnel Interface Src IP/Mask	
这种本地隧道的 IP 地址和子网掩码	
Tunnel Interface Dst IP/Mask	
这种本地隧道的 IP 地址和子网掩码	
Tunnel Based Src IP	
本地网关的 WAN 口地址	
Tunnel Based Dst IP	
远程网关的 WAN 口地址	
Peer IP Address/Mask	
远程网关的子网	
Tunnel Key	
输入隧道的密匙，,仅支持数字，范围是 0 到 4294967296	
Connection Check Interval	
连接检测的时间间隔	0
Connection Check Times	
连续检测到多少次失败后进行重连	3

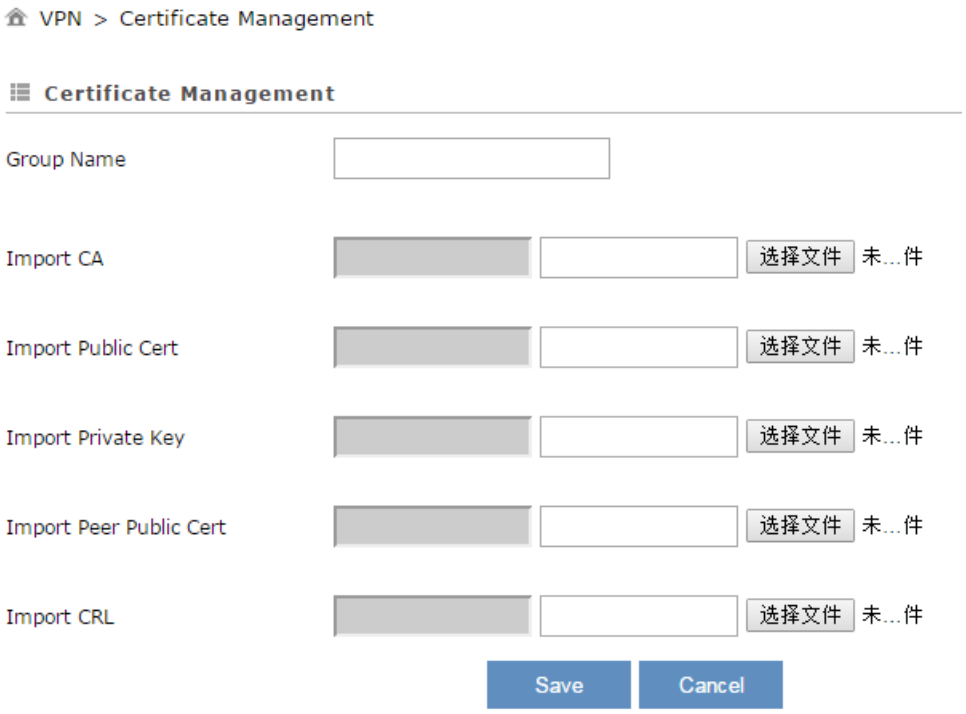
网络拓扑如下:



3.4.6 Certificate 的导入

这个页面用于导入 IPsec 或者 OPENVPN 的证书。

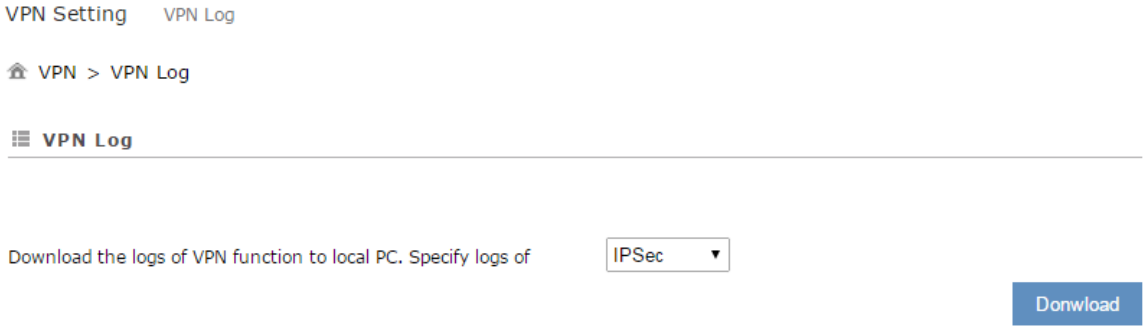




描述	默认值
Group Name	
证书的组名。组名之间的名称不能重复。	
CA	
导入 CA 的的证书文件	
Public Cert	
导入 Public Cert 的证书文件	
Private Cert	
导入 Private certificate 文件	
Peer Public Cert	
导入对端节点的 public certificate 文件	
CRL	
导入证书吊销列表（CRL）	
Password	
输入一个关于证书的携带的密码 Input the password about the certificate file if the file with a password	
Expired Date	
显示证书文件的失效时间	

3.4.7 VPN 日志

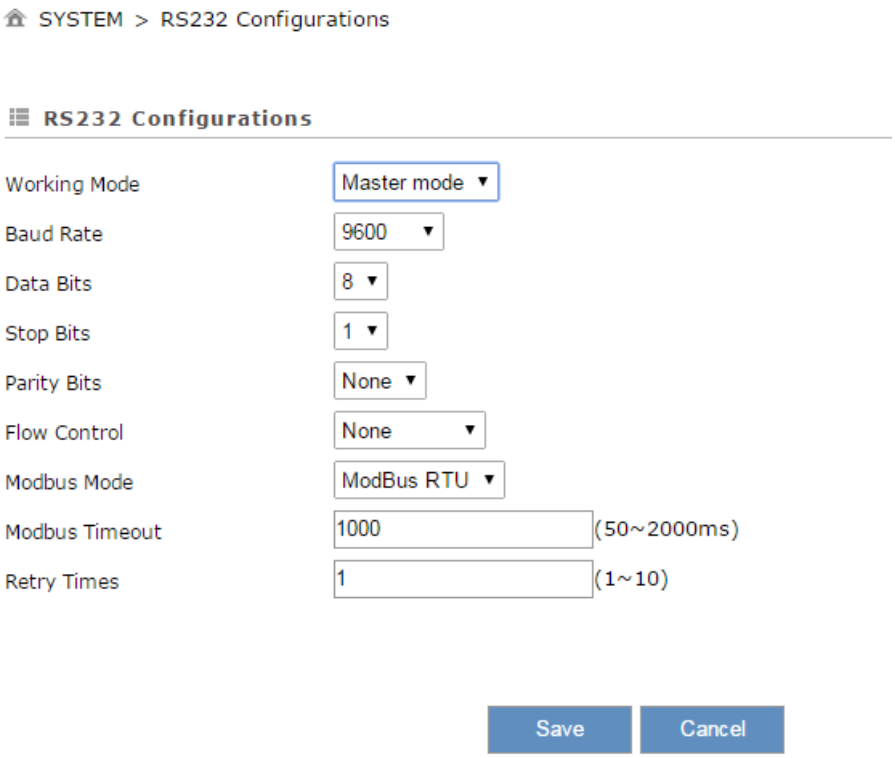
通过这个页面可以下载 VPN 的连接日志。



3.5 接口设置

3.5.1 RS232 设置

VR301 自带一个 5Pin 的的标准 RS232 口。你可以通过下面的页面配置 RS232 的波特率、数据位、停止位等参数。

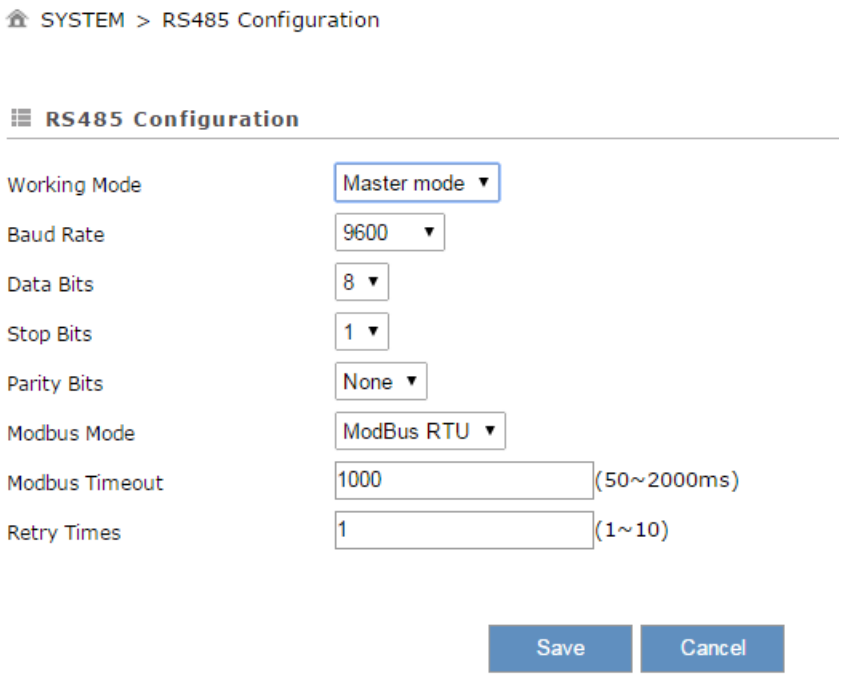


描述	默认值
Working Mode	

描述	默认值
设置 RS232 的工作模式。可以选择主站或者关闭。 ● **Master mode:** DX-3001 将会去读取从站的数据 ● **Close:** 关闭该功能	Close
Baud Rate	
设置 RS232 的波特率.支持的波特率有 2400, 4800, 9600, 19200, 38400, 57600 115200 等。	9600
Data Bits	
设置串口的数据位长度。可以选择 7 或者 8。	8
Stop Bits	
设置串口的 bit 位。可以选择 1 或者 2。	1
Parity Bits	
设置串口的校验位。可以选择 None、Odd、EVEN。	None
Flow Control	
设置串口的流控功能。 可以配置 None、 XON、 XOFF、 RTS、CTS.	None
MODBUS Mode	
设置 MODBUS 通讯的协议。	MODBUS RTU
MODBUS Timeout	
设置 modbus 的通讯超时时间。	1000ms

3.5.2 RS485 设置

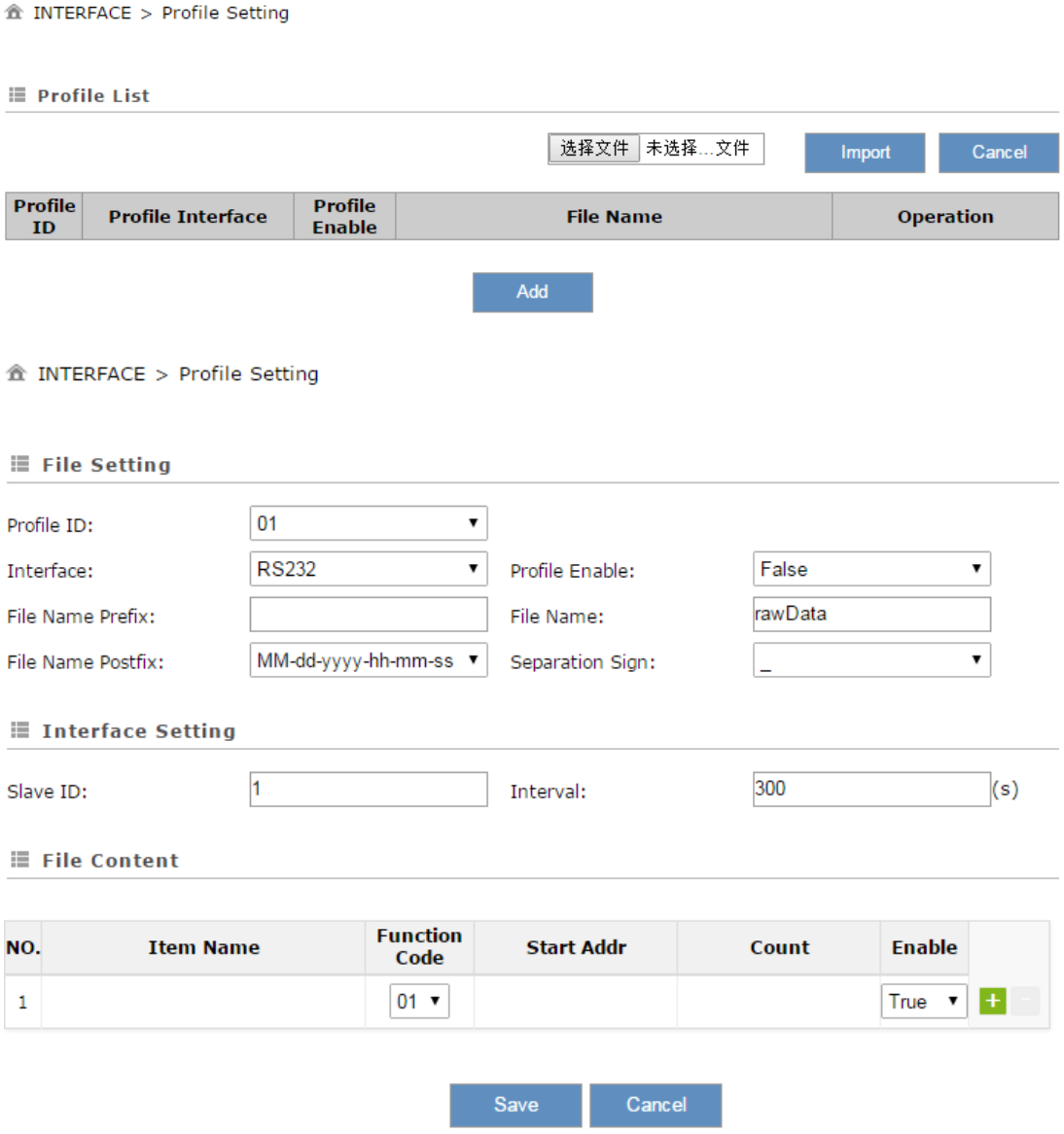
福达 VPN 模块自带一个 RS485 的标准串口。可以通过下面页面对 RS485 进行配置。



Description	Default
Working Mode	
设置 RS232 的工作模式。可以选择主站或者关闭。 ● **Master mode:** DX-3001 将会去读取从站的数据 ● **Close:** 关闭该功能	Close
Baud Rate	
设置 RS232 的波特率.支持的波特率有 2400，4800，9600，19200，38400，57600 115200 等。	9600
Data Bits	
设置串口的数据位长度。可以选择 7 或者 8。	8
Stop Bits	
设置串口的 bit 位。可以选择 1 或者 2。	1
Parity Bits	
设置串口的校验位。可以选择 None、Odd、EVEN。	None
MODBUS Mode	
设置 MODBUS 通讯的协议。	MODBUS RTU
MODBUS Timeout	
设置 modbus 的通讯超时时间。	1000ms

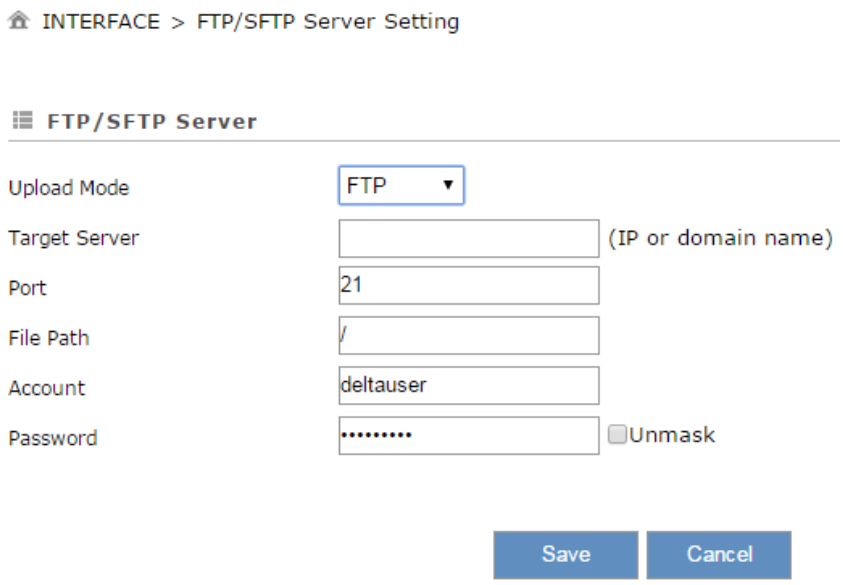
3.5.3 Profile Management（采集地址配置）

通过下面的页面可以进行配置采集的点位。



3.5.4 FTP/SFTP Server 设定

上面数据采集的文件需要指定一个 FTP 或者 SFTP 服务器。这样就能实现数据采集。用户可以通过如下页面进行配置。



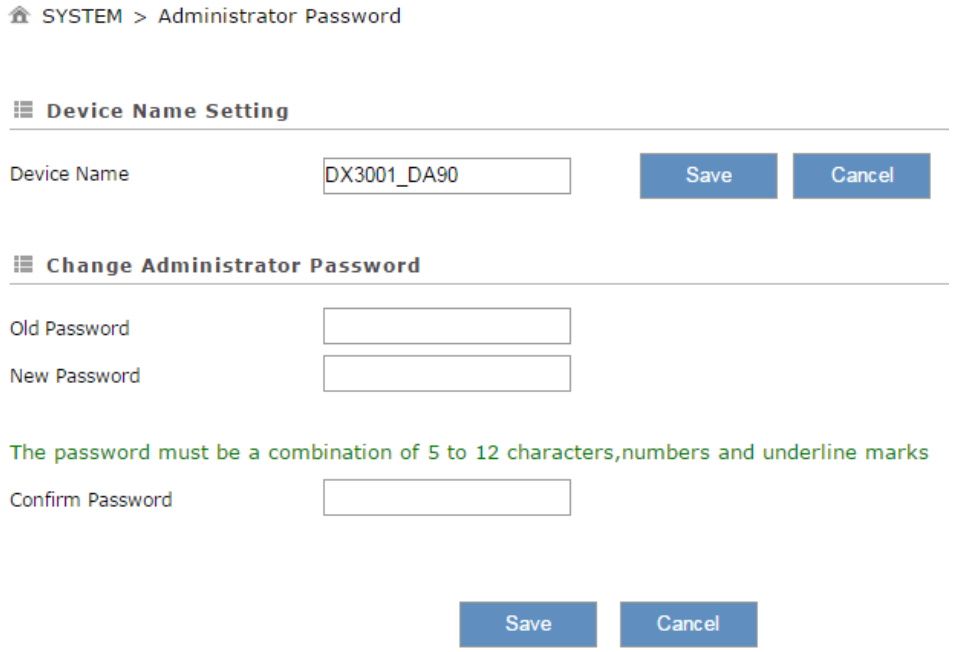
Description	Default
Upload Mode	
上传模式的选择。 可以关闭或者选择 FTP、SFTP	Disabled
Target Server	
设置 FTP/SFTP 服务器的 IP 或者域名	
Port	
设置服务器的监听端口	
File Path	
设置服务器的上传路径	/
Account	
设置 FTP/SFTP 服服务器的认证用户名	
Password	
设置 FTP/SFTP 服服务器的认证密码	

3.6 System

你能够在通过系统配置页面，进行设备管理、时间配置、固件升级、配置备份和恢复、系统重启、SD 卡管理、网络诊断等功能。

3.6.1 Name and Password

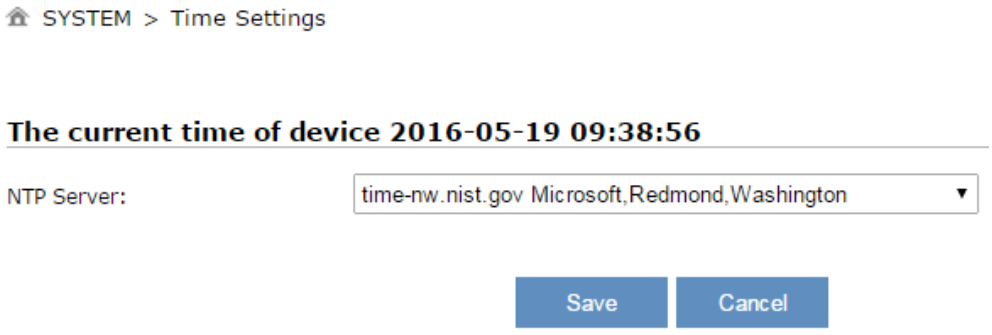
通过这个页面可以修改路由器的名称和访问密码。密码只能是 5~12 位的数字或者字母下划线。



描述	默认值
Device Name	
输入您需要的设定的设备名称	型号 + “_” + “MAC 地址后四位”
Old Password	
输入登录的旧密码	admin
New Password	
输入您需要更改的密码。面只能是 5~12 位的字符或者数字的组合。	N/A
Confirm Password	
再次输入您需要更改的密码。	A/A

3.6.2 NTP Server 设置

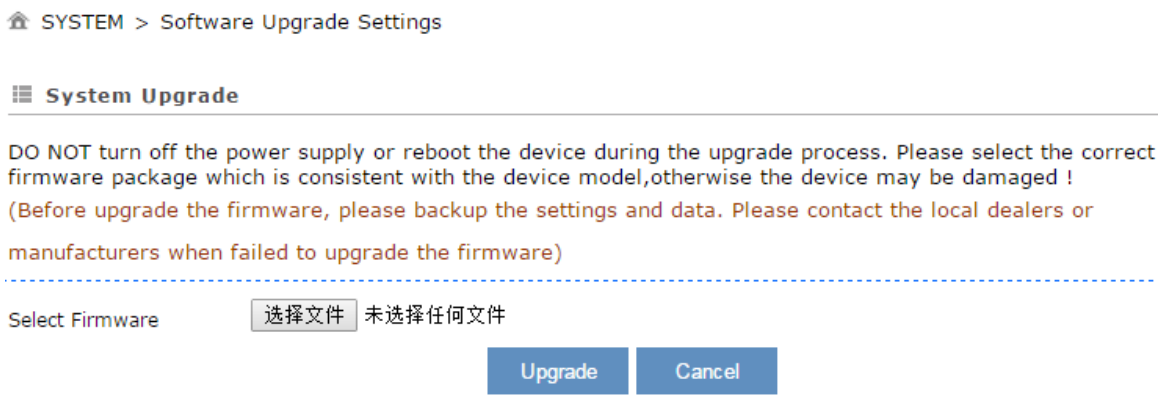
通这个页面，可以配置 NTP 服务器的时区或者 NTP 服务器。



Description	Default
The current time of device	
显示设备的当前时间	N/A
NTP Server	
选择路由器工作的时区，GMT-12：00 至 GMT+13：00	N/A
Main NTP Server	
当选择 others 的时候需要手动设 NTP 的服务的域名或者 IP	N/A
Backup NTP Server	
当选择 others 的时候需要手动设备用 NTP 的服务的域名或者 IP	N/A

3.6.3 Firmware Upgrade（固件升级）

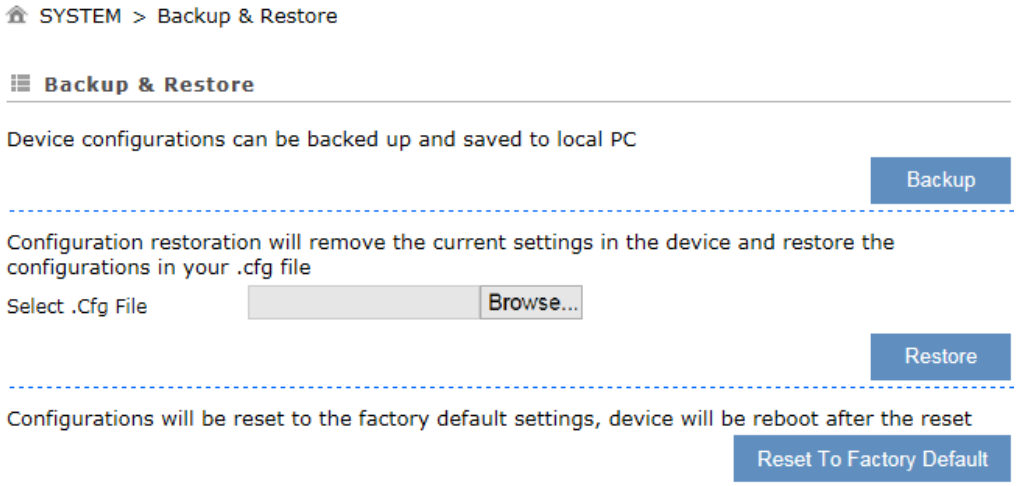
通过下面这个页面可以进行固件的升级。



描述	默认值
Chose file	
点击在“选择文件“ 选择需要升级的 bin 文件	N/A
Upgrade	
点击 “Upgrade”会进行升级。升级过程中请勿断电。过程大约会持续 5min。期间会自动重启。	N/A

3.6.4 Backup & Restore（配置备份和恢复）

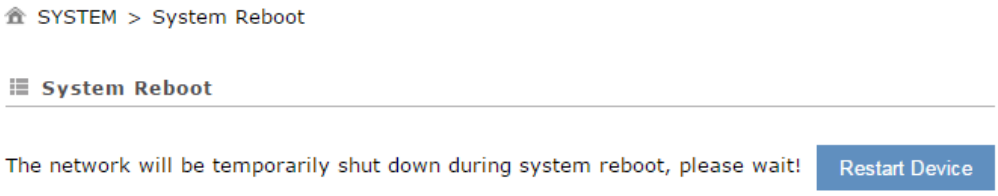
通过这个页面可以导入之前的配置文件或者导出当前的配置。



描述	默认值
Backup	
点击“Backup”备份当前路由器配置信息。	N/A
Restore	
使用之前备份的配置文件恢复路由器配置信息。	N/A
Restore To Factory Default	
恢复路由器出厂设置信息。	N/A

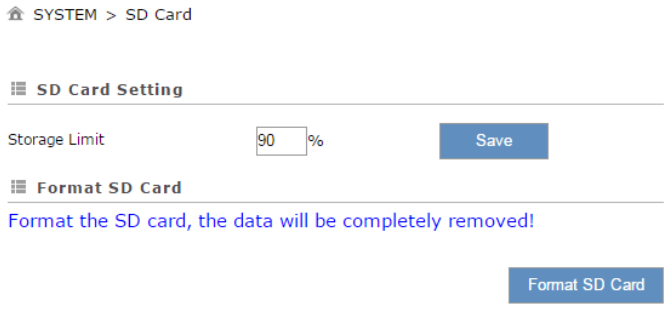
3.6.5 System Reboot

用户可以通过该功能手动重启路由器



3.6.6 SD Card

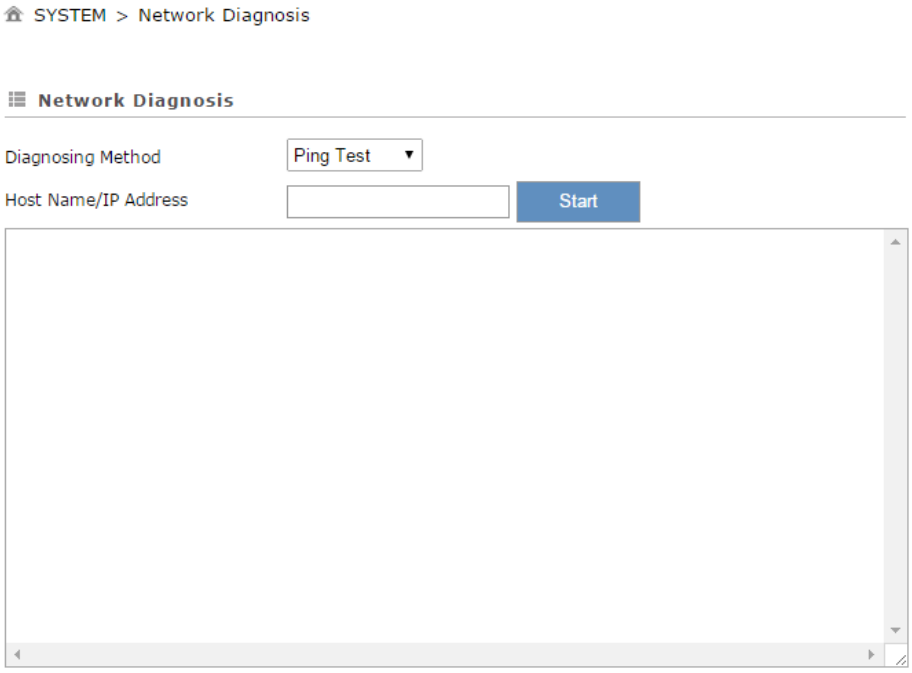
用户可以通过改页面对 SD 卡进行管理



描述	默认值
Storage Limit	
设置存储限制。到指定数据容量后，旧的数据将会被新的数据覆盖。	90%
Format SD Card	
点击该按钮可以进行 SD 卡的格式化	N/A

3.6.7 Network Diagnosis

本页主要用于诊断路由器基本网络故障。



Description	Default
Diagnosing Method	
选择诊断类型，可选值为“Ping Test”，“Route Trace”。	Ping Test
Host Name/IP Address	
输入检测的域名或者 IP 地址	N/A
Start	
点击“Start”按钮进行诊断	N/A

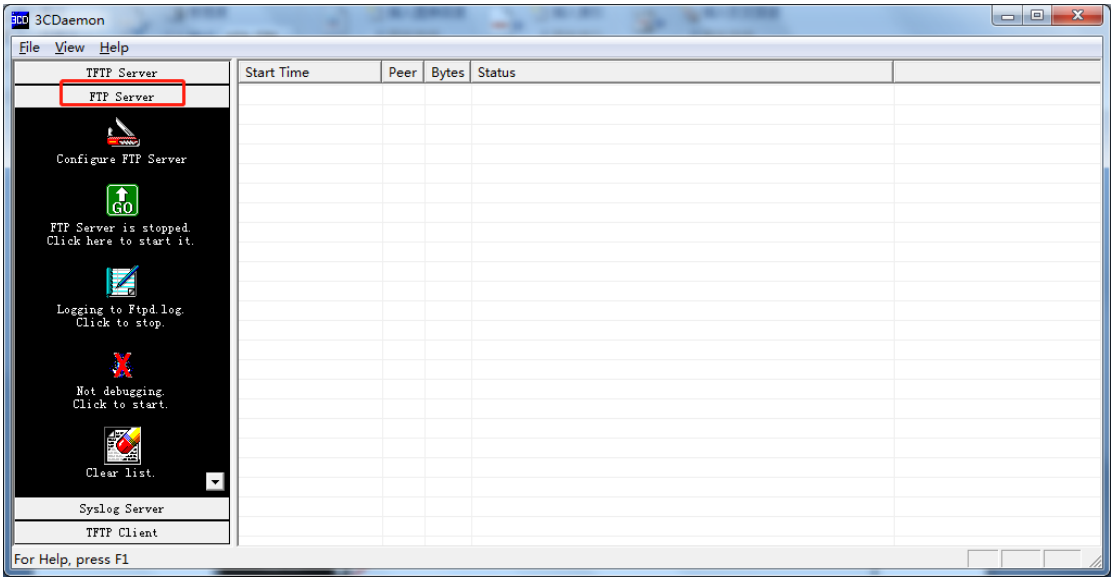
第四章 应用教程

4.1 通过 FTP Server 收集 VR301 采集的数据

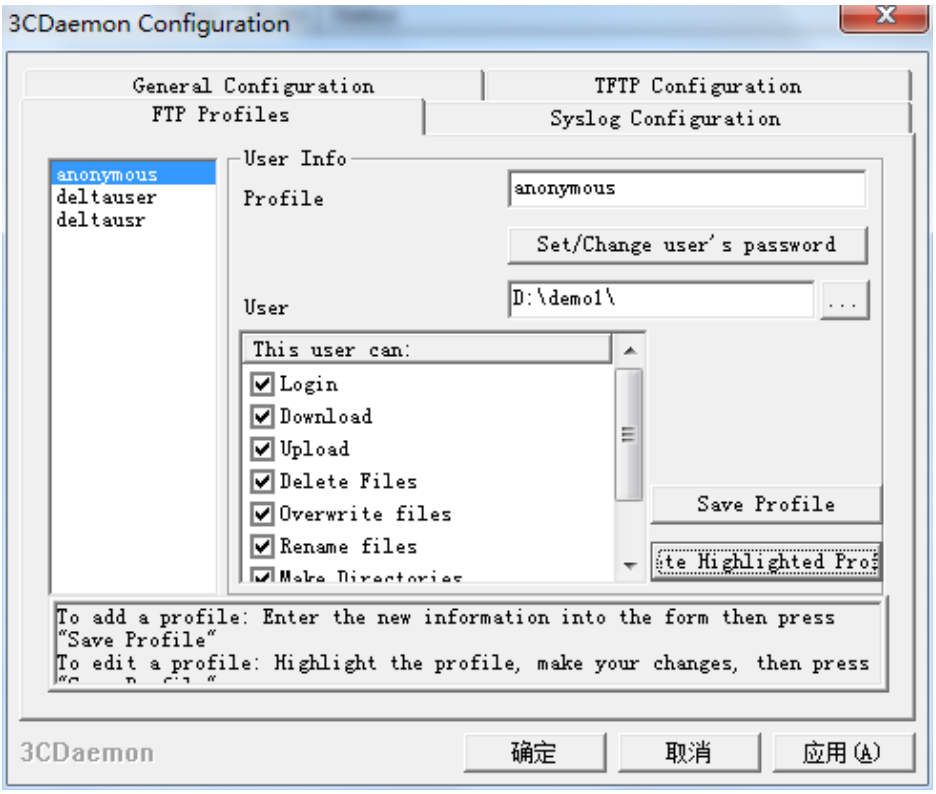
场景：VR301 通过 MODBUS TCP 协议采集 PLC 的协议。VR301 将采集到数据生成 CSV 文档，通过 FTP 上传上传到 FTP 的服务器。PLC 的 IP，192.168.1.5；VR301 的 IP，192.168.1.1；服务器 IP192.168.1.100。

由于数据采集生成的文档，需要通过 FTP Server 或者 SFTP Server 来进行接收。所以在这里，我们利用 3CDaemon 来进行 FTP 服务器的搭建。

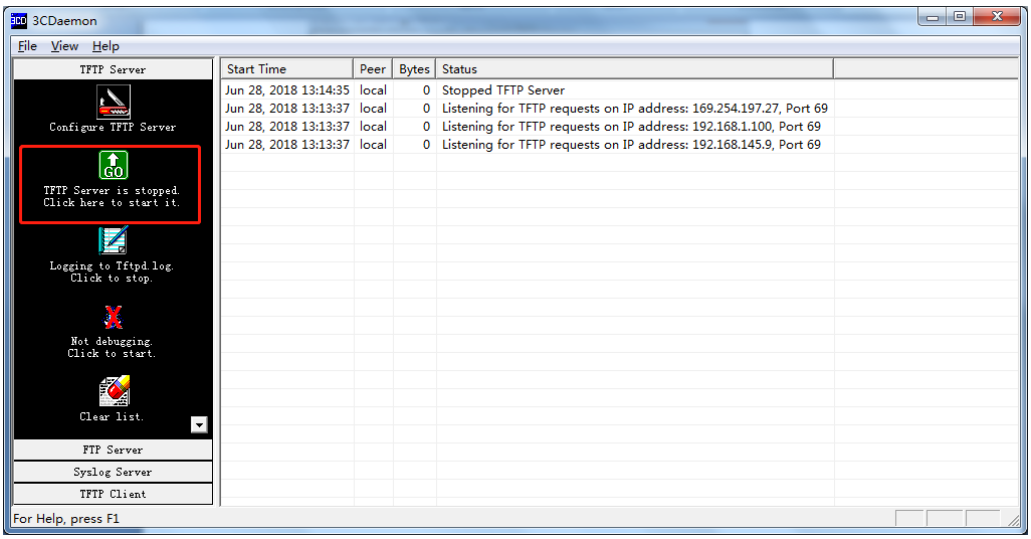
打开 3CDaemon 来进行设定。在下面的介绍中，以 FTP 为例。



点击 TFTP Server 下的“Config FTP Server”，进行存储路径配置

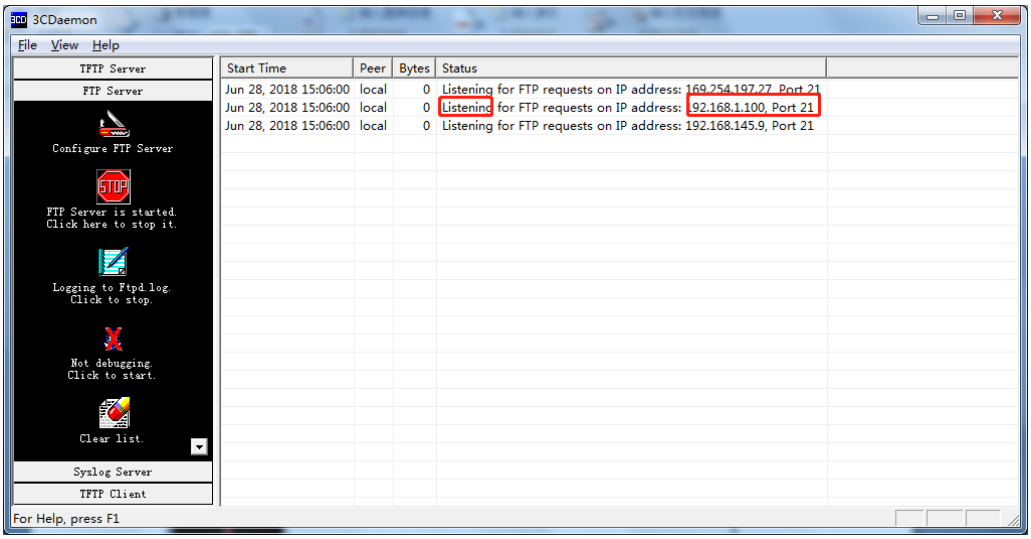


配完成后点击应用，然后返回到主界面。点击  启动 FTP 服务。

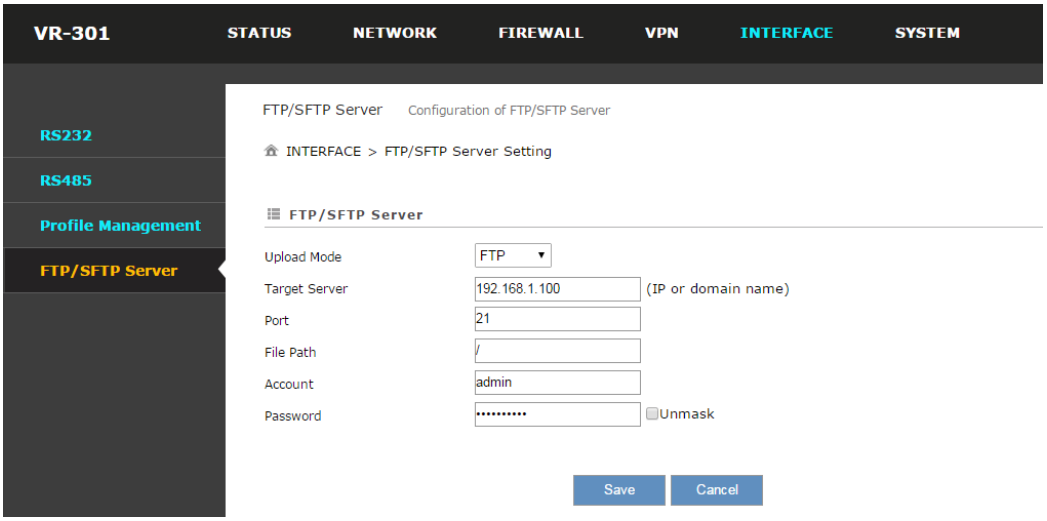


注：有些时候服务的监听端口会被防火墙挡住，最好在防火墙关闭的情况下测试。

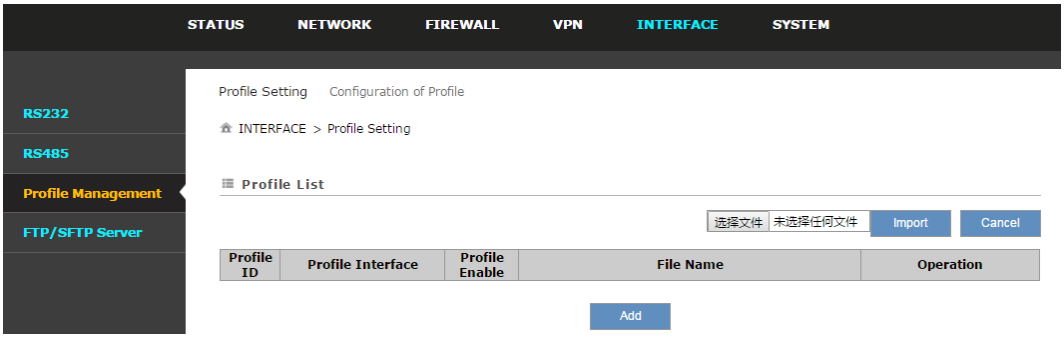
当启用成功后将旁边的日志将会显示如下：



设置 DX301 内部 TFTP 配置。配置完成后点击【Save】



配置 Profile 的应用



点击“ADD”按钮。设置 modbus TCP 的资料的采集资料如下。

Profile Setting Configuration of Profile

INTERFACE > Profile Setting

File Setting

Profile ID: 01

Interface: LAN.Modbus.TCP.Mas Profile Enable: True

File Name Prefix: modbusTCP File Name: TCPdata

File Name Postfix: Unix Timestamp Separation Sign: _

Interface Setting

Target IP Address: 192.168.1.5 Port: 502

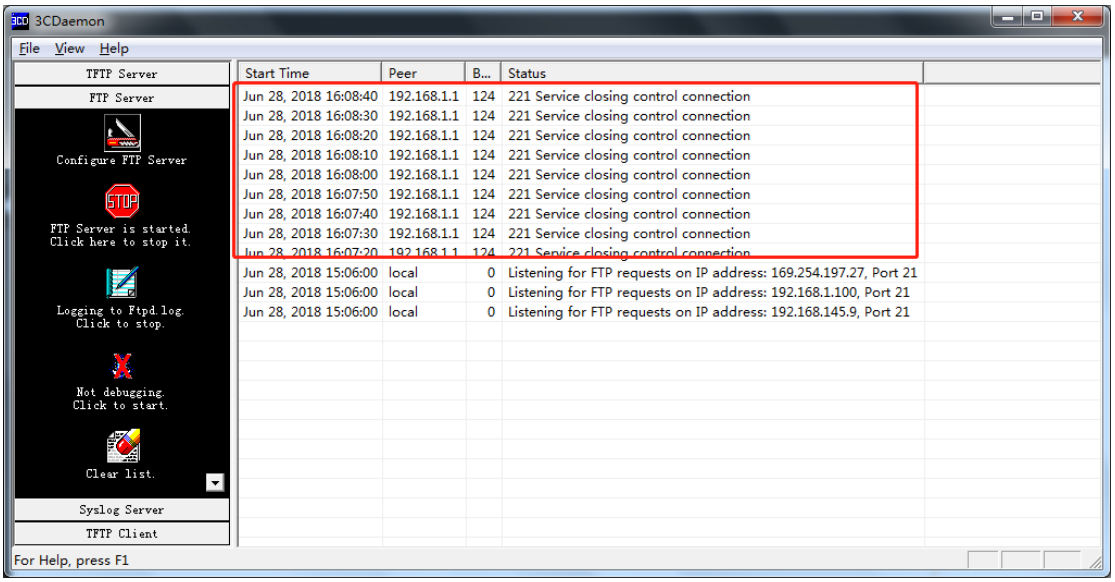
Interval: 300 (s)

File Content

NO.	Slave ID	Item Name	Function Code	Start Addr	Count	Enable
1	1	test1	01	0	10	True
2	1	test2	01	10	20	True

Save Cancel

当采集到数据后，就会自动生成 CSV 文档传到 FTPserver 上。此时会出现如下的日志：



打开文件对应路径的文件可以看到 ftp 服务器端收到文件列表

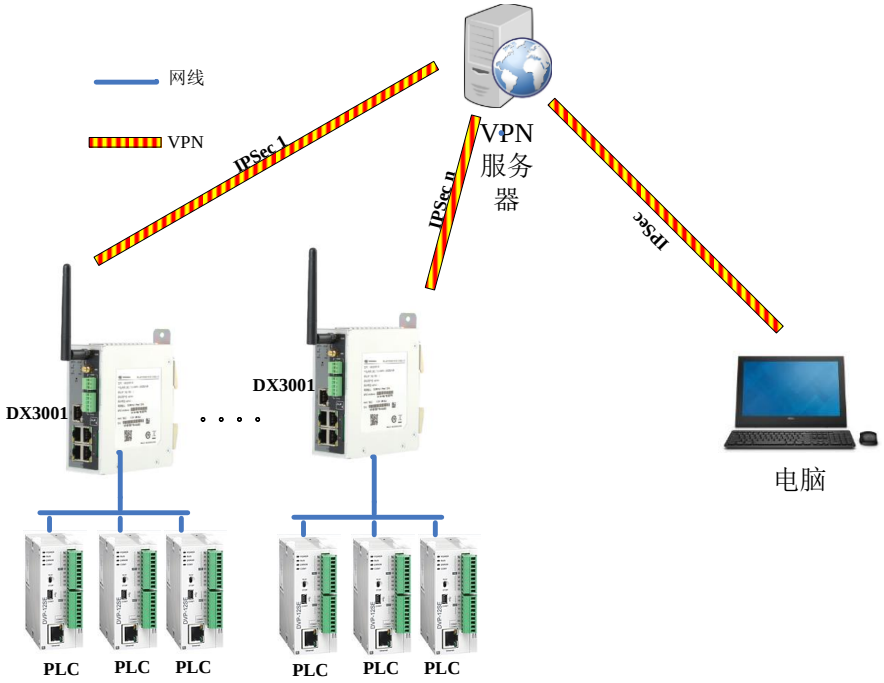
modbusTCP#TCPdata#1530173238.csv	2018-06-28 16:07	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173248.csv	2018-06-28 16:07	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173258.csv	2018-06-28 16:07	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173268.csv	2018-06-28 16:07	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173278.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173288.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173298.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173308.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173318.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173328.csv	2018-06-28 16:08	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173338.csv	2018-06-28 16:09	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173348.csv	2018-06-28 16:09	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173358.csv	2018-06-28 16:09	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173368.csv	2018-06-28 16:09	Microsoft Office...	1 KB
modbusTCP#TCPdata#1530173378.csv	2018-06-28 16:09	Microsoft Office...	1 KB

打开 csv 文档后可以看到：item 的名称，item 中的数据和采集的时间戳。

A	B	C
test1	0 0 0 0 0 0 0 0 0 0	2018-6-28 8:07
test2	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	2018-6-28 8:07

4.2 IPSec 的应用场景

通过在 VPN 服务器建立多条 IPsec 的通道。VPN 服务器可以和各个现场进行通信。当人员不在公司的时候，可以通过远程 VPN 连到服务器，利用远程桌面等，进行数据查看。

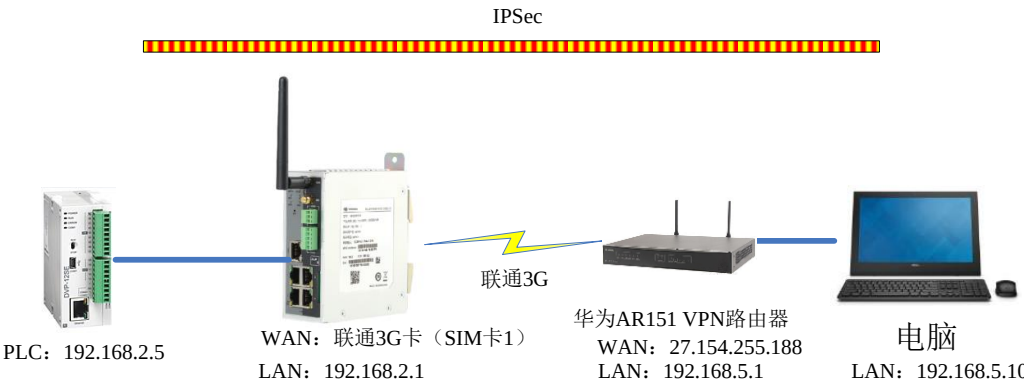


（注：一个 VPN 通道对应一个 IPSec 的连接。每个现场需要占用一个 IPsec 的连接。服务器所支持的连接数由服务器本身的性能决定，具体参数请咨询相关厂家。）

在这里我们模拟一其中一个连接的建立的过程。VPN 服务器采用的是华为 AR151W-P-S，

VPN 的客户端使用的是 VR301 的工业级路由器。

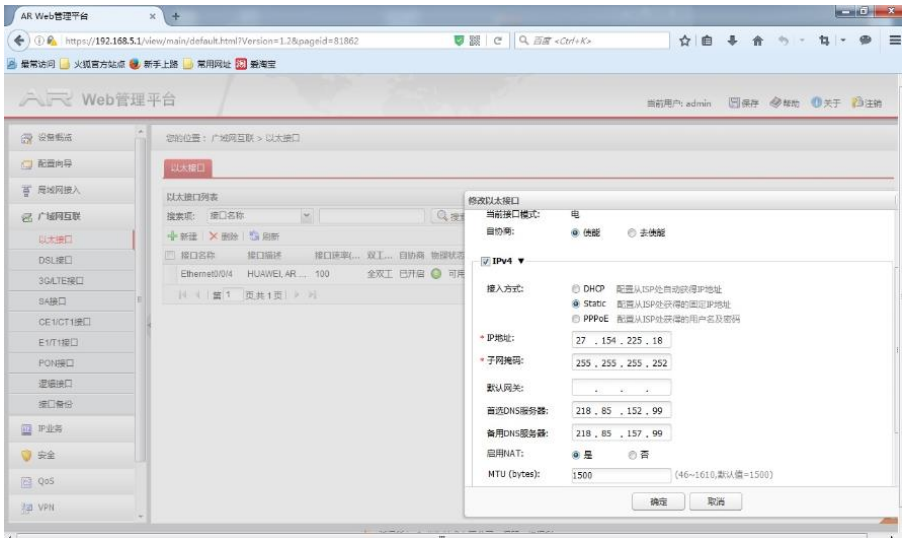
组网示意图如下：



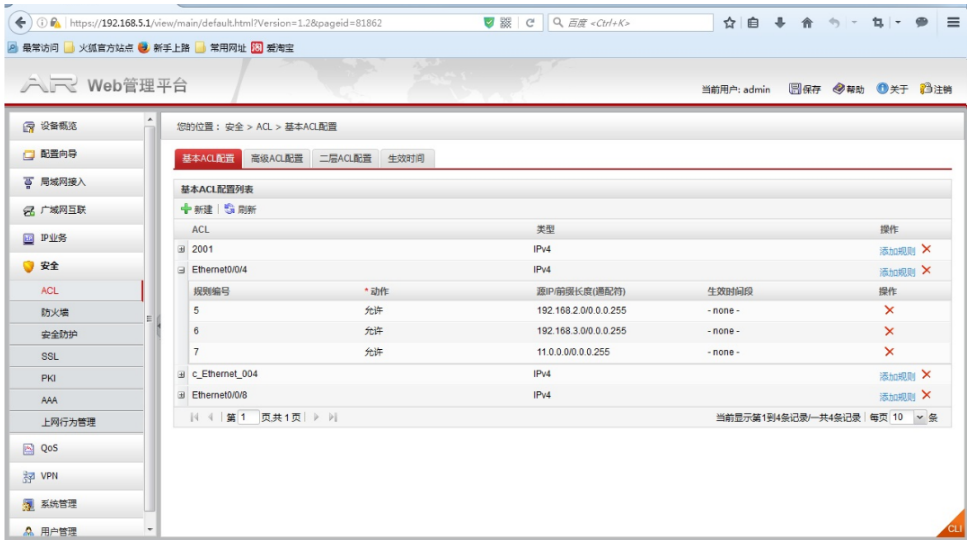
配置如下：

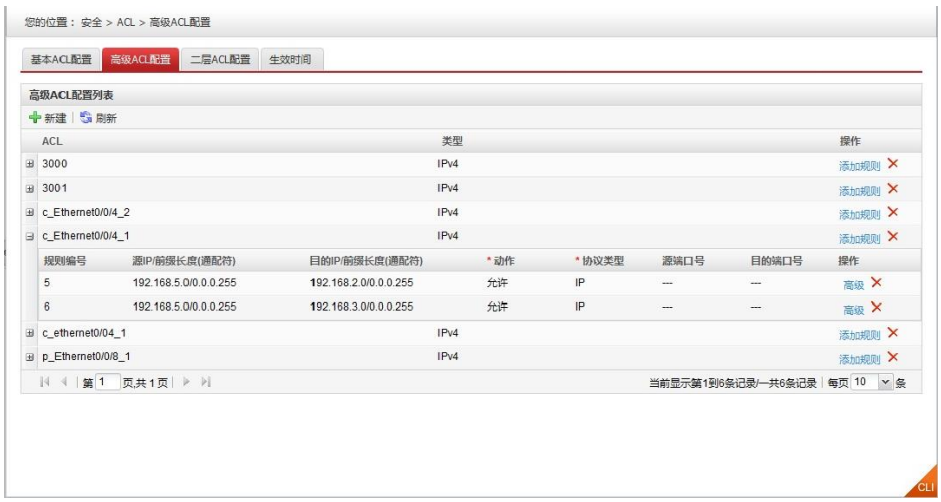
1. 配置华为的 VPN 路由器，过程如下：

（1） 配置 VPN 服务器的 WAN 口 IP



（2） 配置 ACL 过程，允许 192.168.2.0/24 网段的 IP 通过

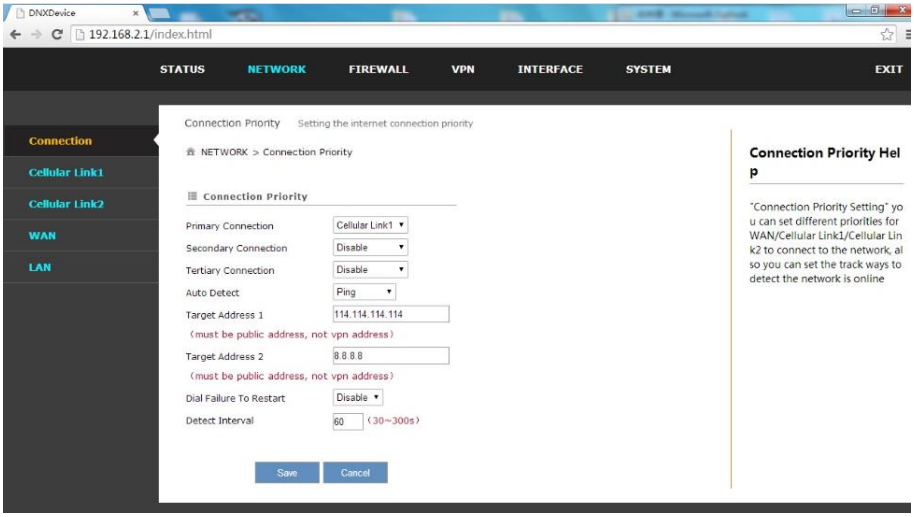




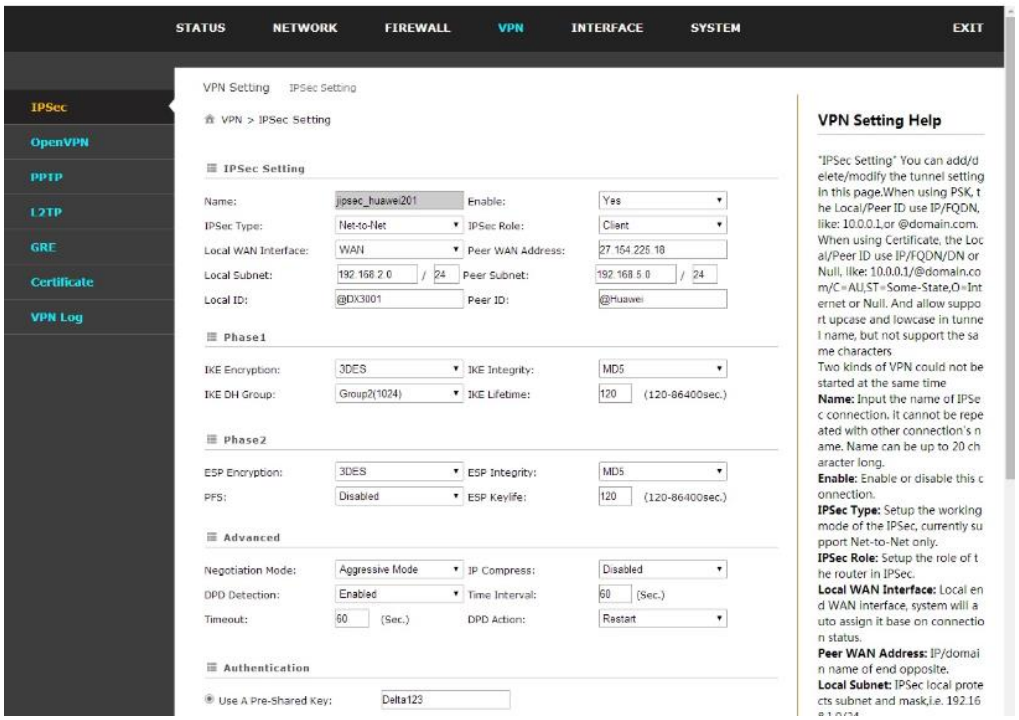
（3） 配置 IPSec 服务器端的配置

2. VR301 的配置

（1） 设置 WAN 口的连接为 SIM1



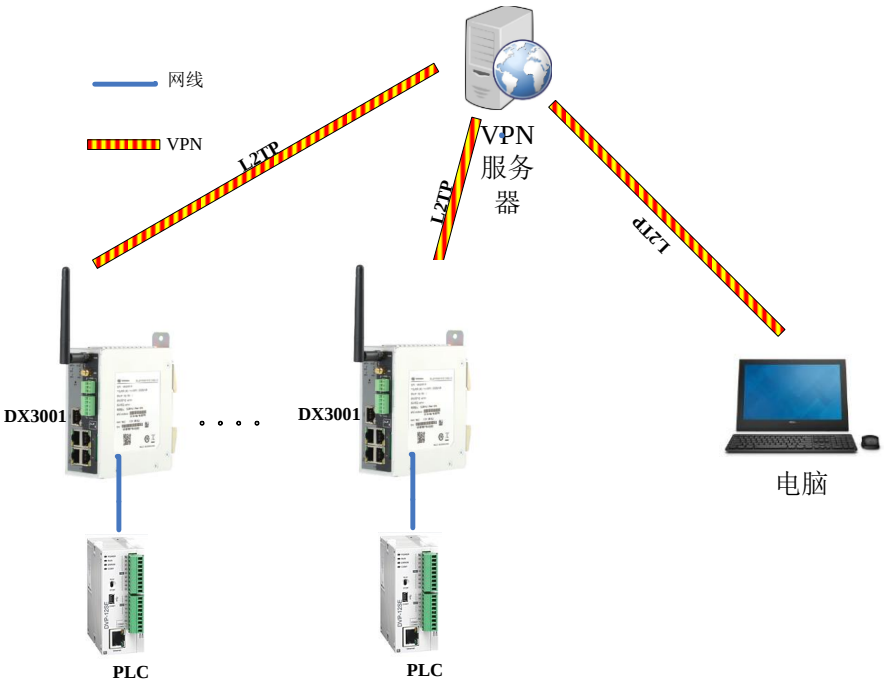
（2） 配置 VR301 内部的 VPN 策略



到此配置完成，就可以做测试了。

4.3 L2TP 配置场景

通过架设一个 L2TP 服务器，设置一次 L2TP 服务器策略就能支持多个 L2TP 的客户端连接过来，具体能够支持多少个 L2TP 的连接看 L2TP 服务器的性能决定，具体可以查询相关手册。

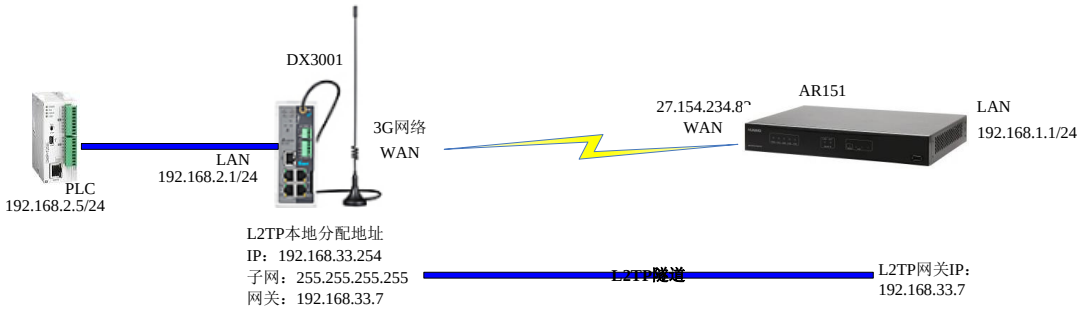


由于 L2TP 在连接的时候，L2TP 服务器会给其分配一个 IP，这是一个虚拟的 WAN 口 IP。所有虚拟的 WAN 口 IP 之间是互通。L2TP 客户端中可以使用 DMZ，端口映射等就可以访问

到 PLC。这样电脑如果运行一个 L2TP 客户端与服务器建立好连接就能够直接访问各个现场的 PLC，这样不用像 IPsec 一样需要远程登录到服务器才能访问 PLC。

在这里我们使用华为的 AR151 的 VPN 路由器作为测试环境。

网络拓扑



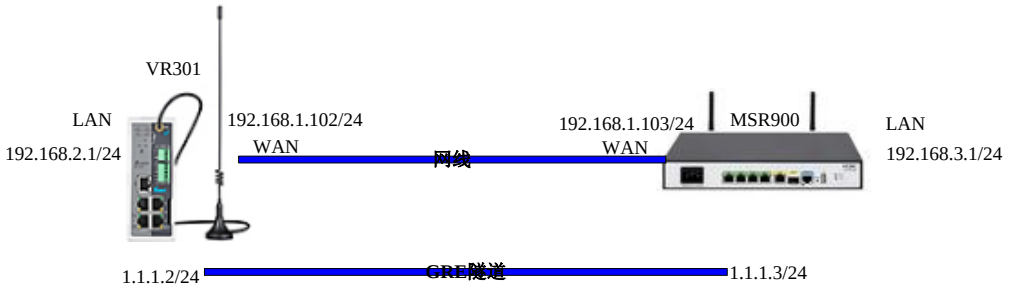
VPN 的具体配置参照 VR301 与华为 AR151 的 L2TP 配置的章节。

第五章 VR301 与第三方 VPN 路由器对接配置

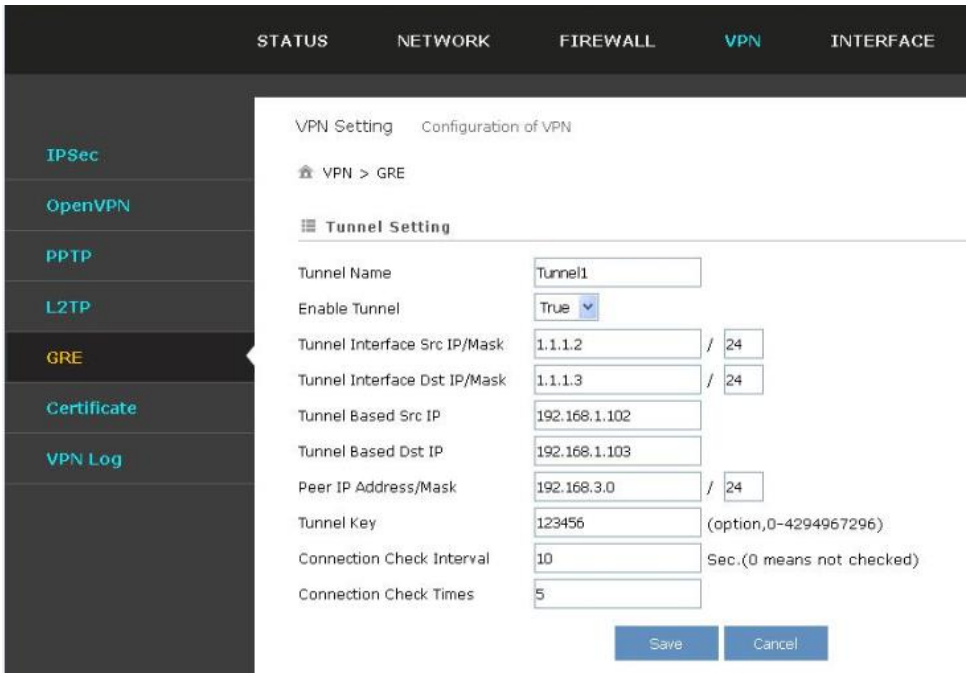
5.1 华为 VPN 路由器与 VR301 的配置

5.1.1 华为 MSR900 与 VR301 的 GRE（带隧道密匙）配置

网络拓扑

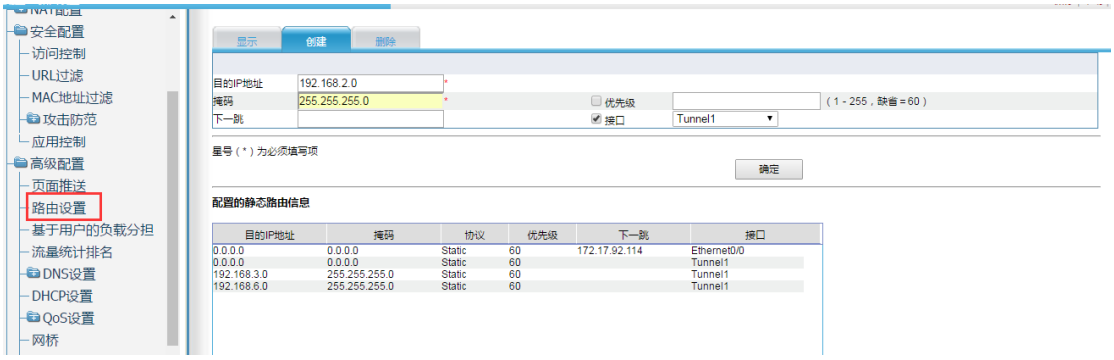


VR301 端的 GRE 配置如下



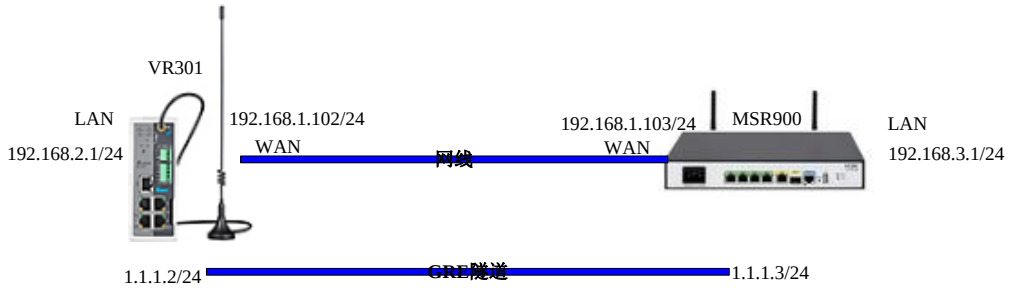
华为 MSR900 的 GRE 配置如下：

此时是可以 GRE 的隧道已经打通，但是 MSR900 的 lan 口和 GRE 的 LAN 依然不能相互通信。如果需要通讯需要新加一条路由，目的 IP 地址即为 VR301 的网段，接口选择 GRE 的隧道名称。（VR301 内部的路由在配置完 GRE 的时候已经自动生成）

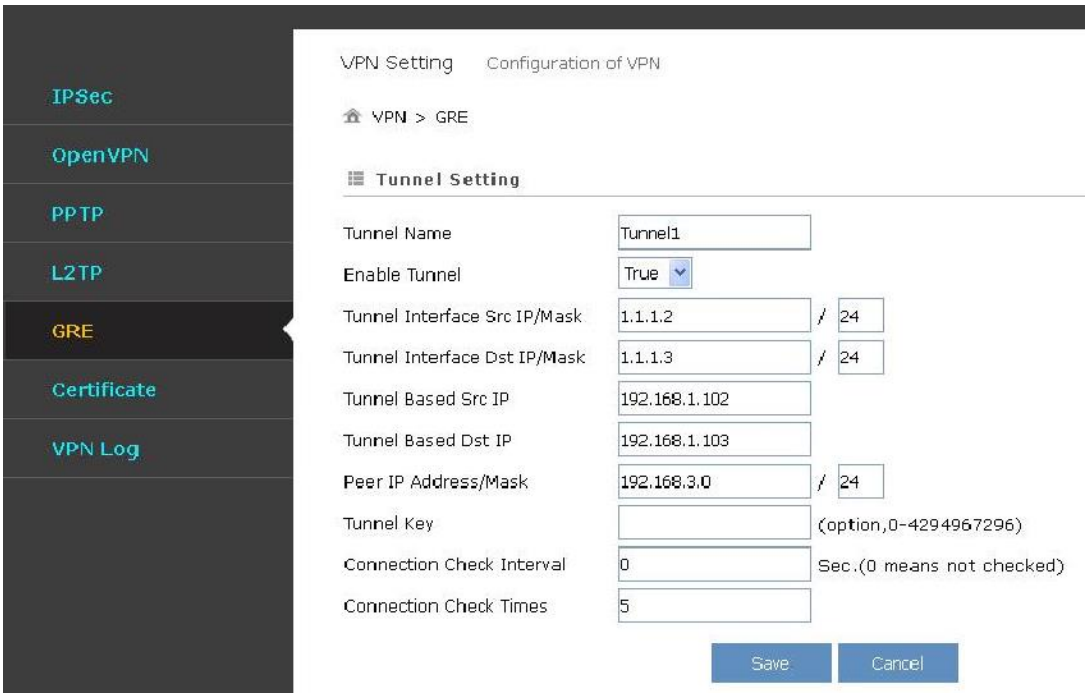


5.1.2 华为 MSR900 与 VR301 的 GRE（不带隧道密匙）配置

网络拓扑

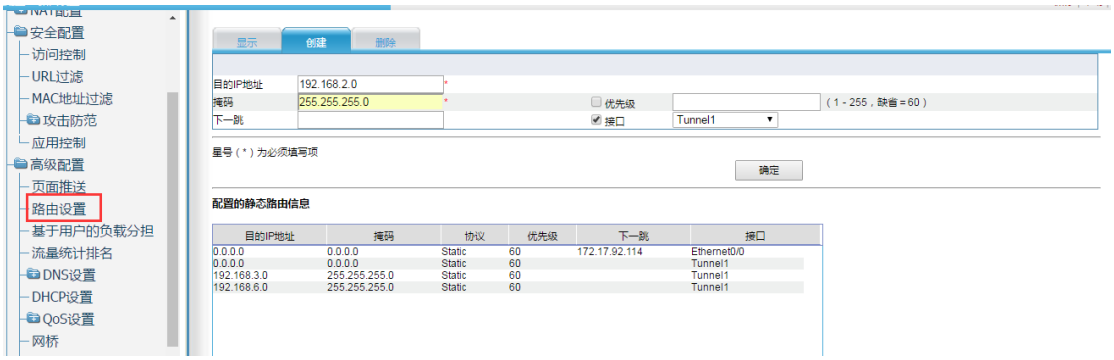


VR301 端的 GRE 配置如下



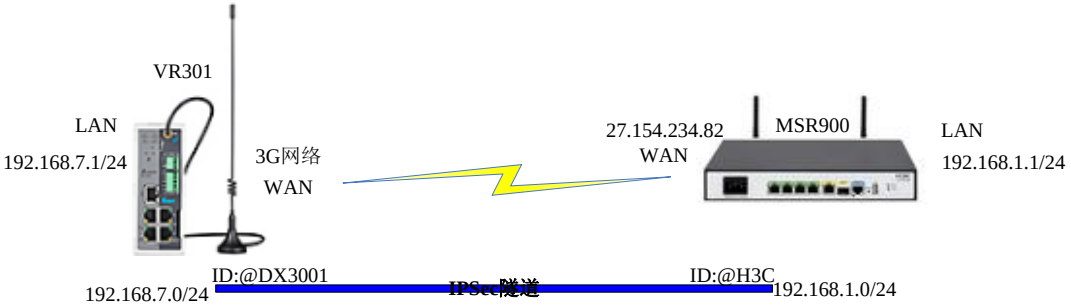
MSR900 的 GRE 的配置如下：

此时是可以 GRE 的隧道已经打通，但是 MSR900 的 lan 口和 GRE 的 LAN 依然不能相互通信。如果需要通讯需要新加一条路由，目的 IP 地址即为 VR301 的网段，接口选择 GRE 的隧道名称。（VR301 内部的路由在配置完 GRE 的时候已经自动生成）

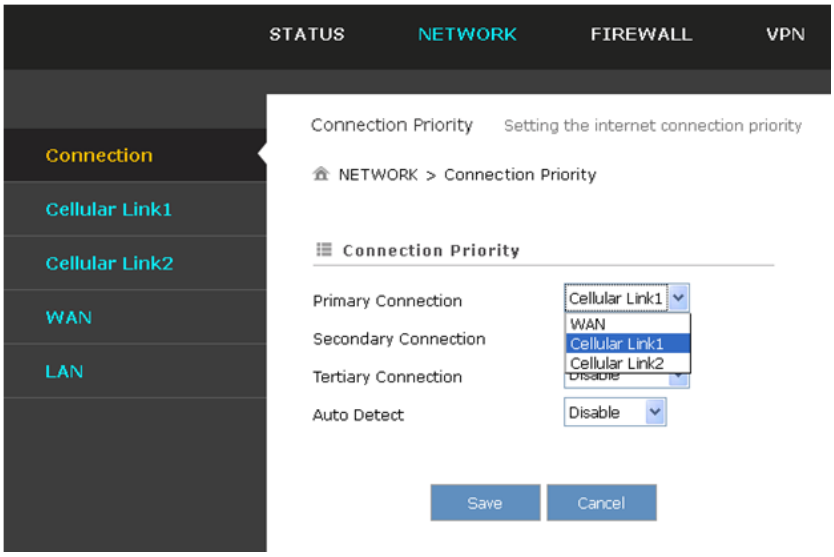


5.1.3 华为 MSR900 与 VR301 的 IPSec（PSK 方式）配置

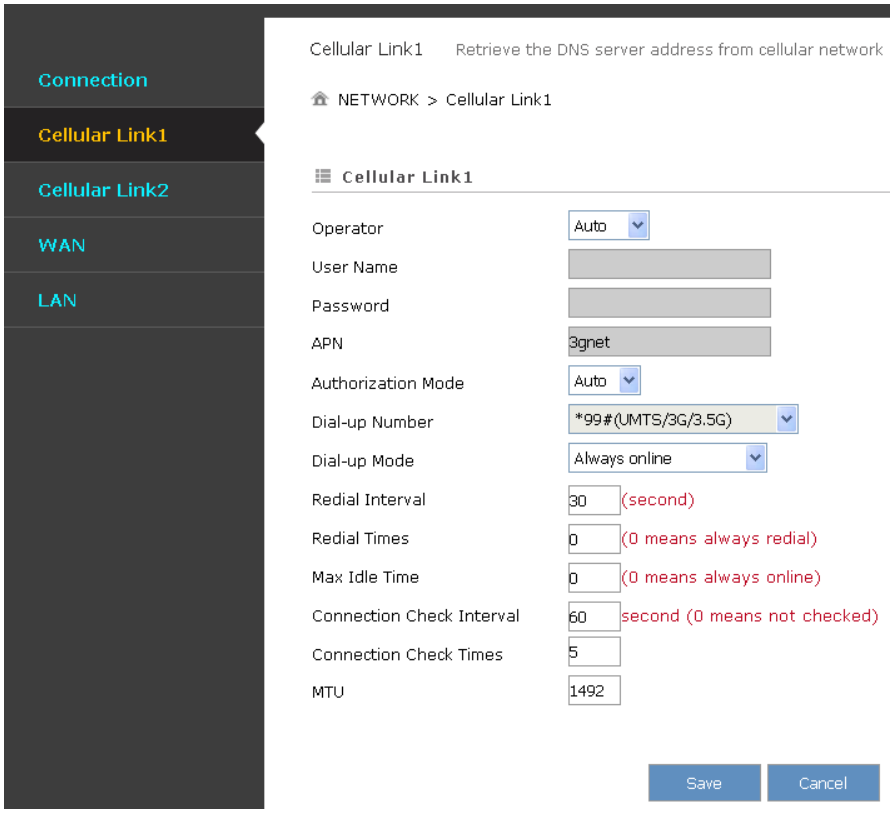
网络拓扑



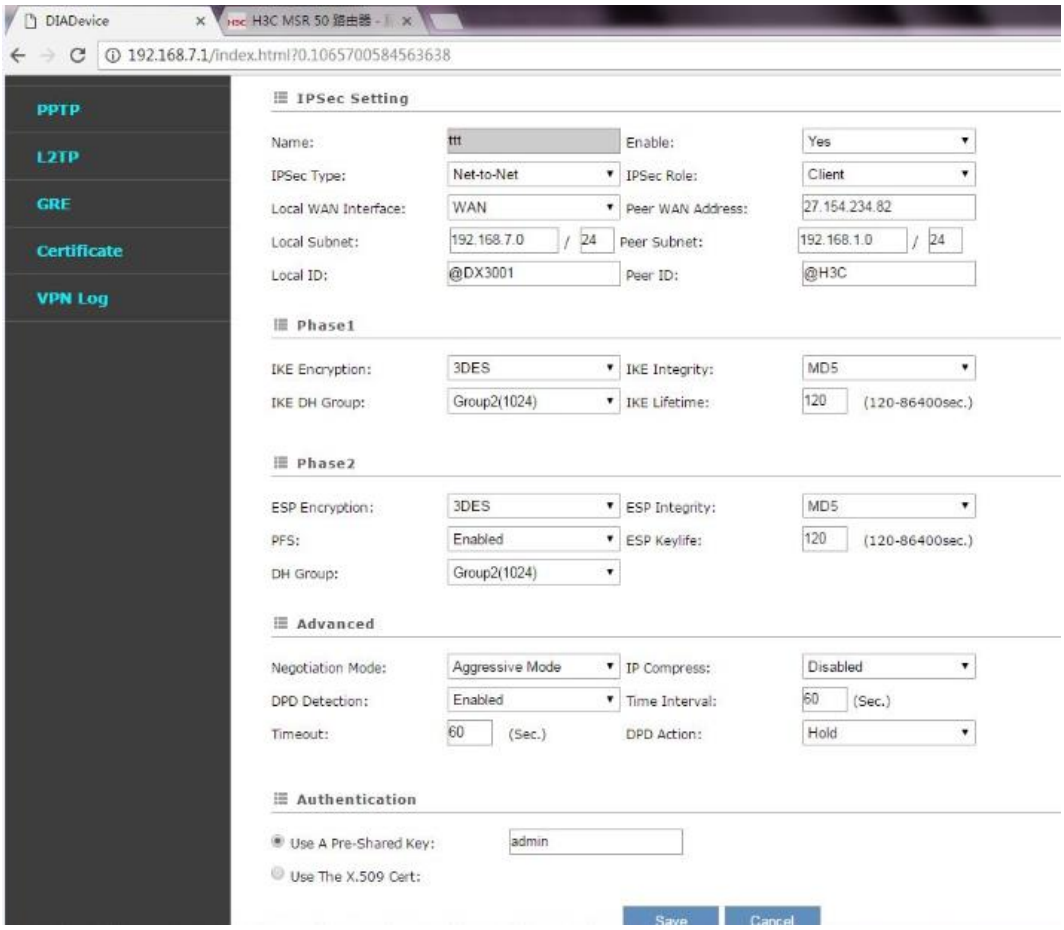
VR301 的设置通过 SIM1 来上网



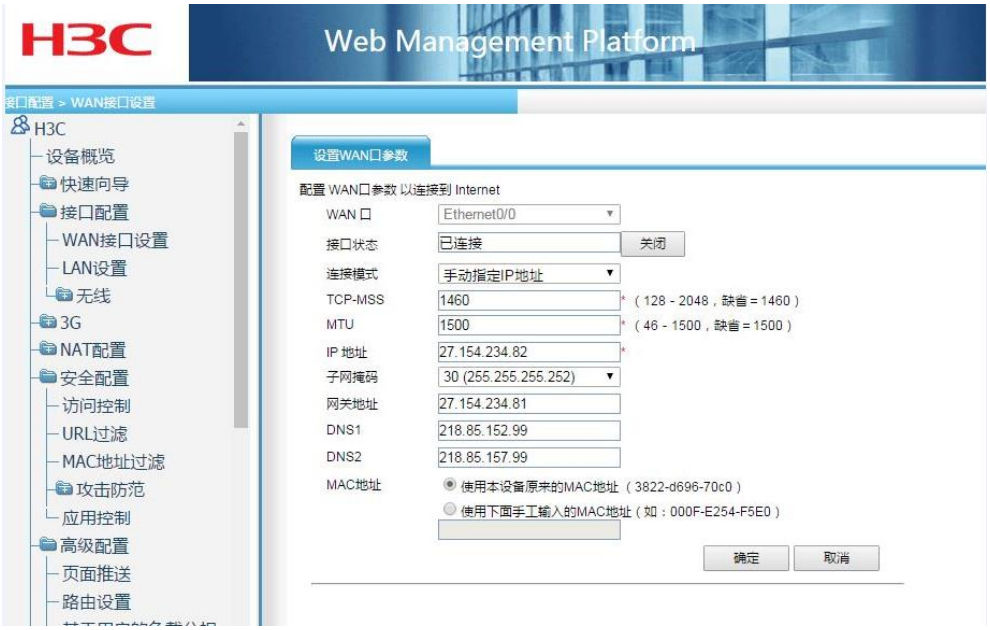
配置 SIM1 的 APN 参数



设置 VR301 的 IPSec 参数



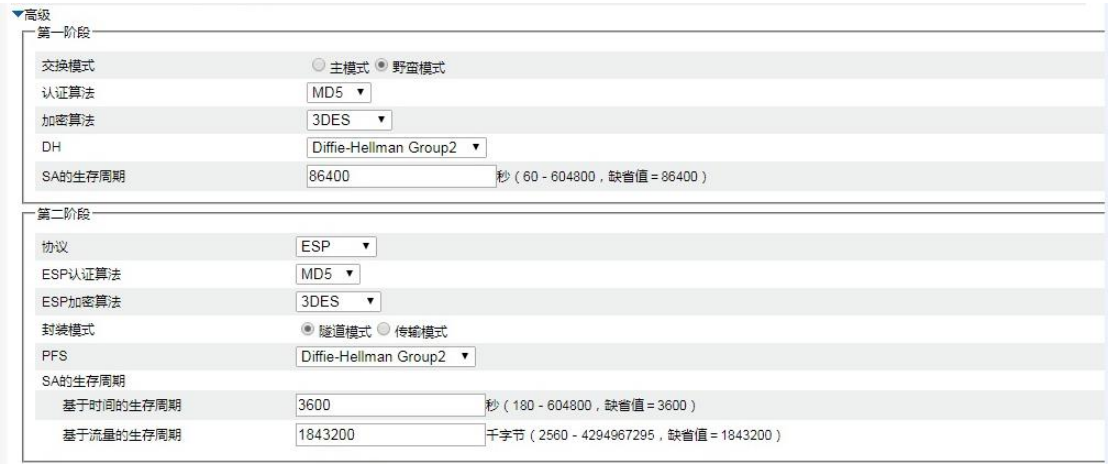
配置 MSR900 的 WAN 口参数



MSR900 的隧道配置截图 1

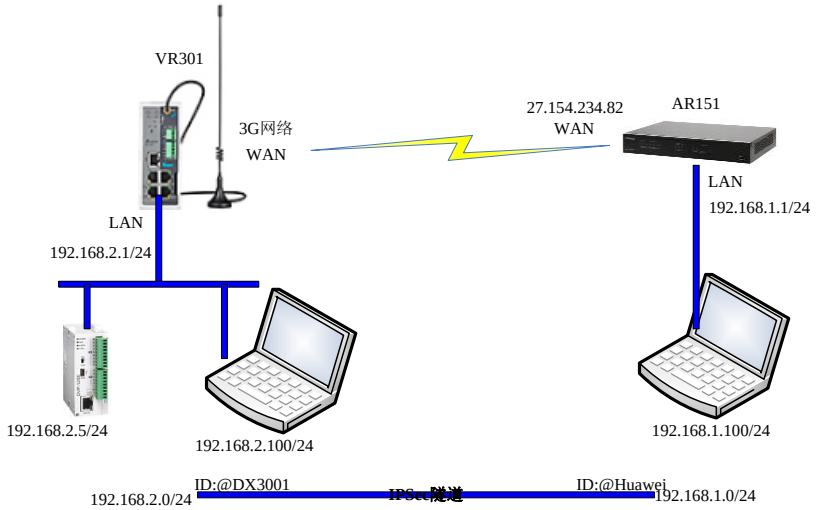
MSR900 的隧道配置截图 2

MSR900 的隧道配置截图 3

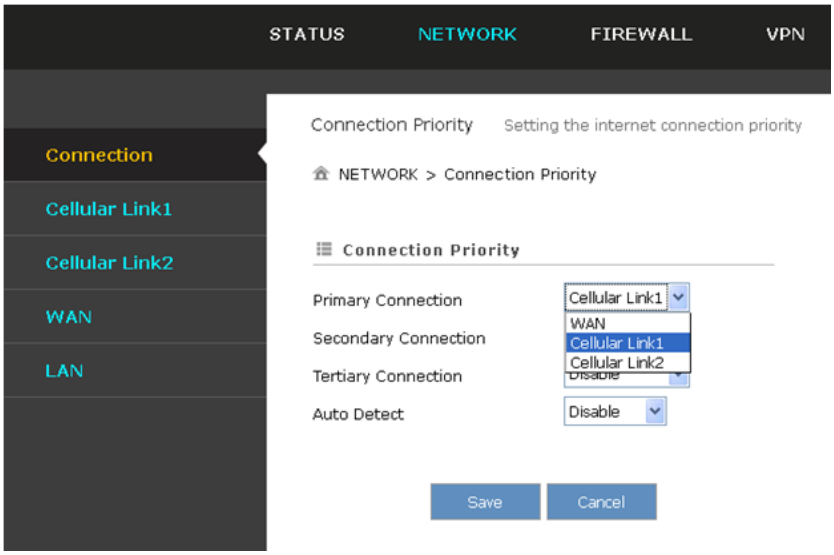


5.1.5 华为 AR151 与 VR301 的 Ipsec（PSK）配置

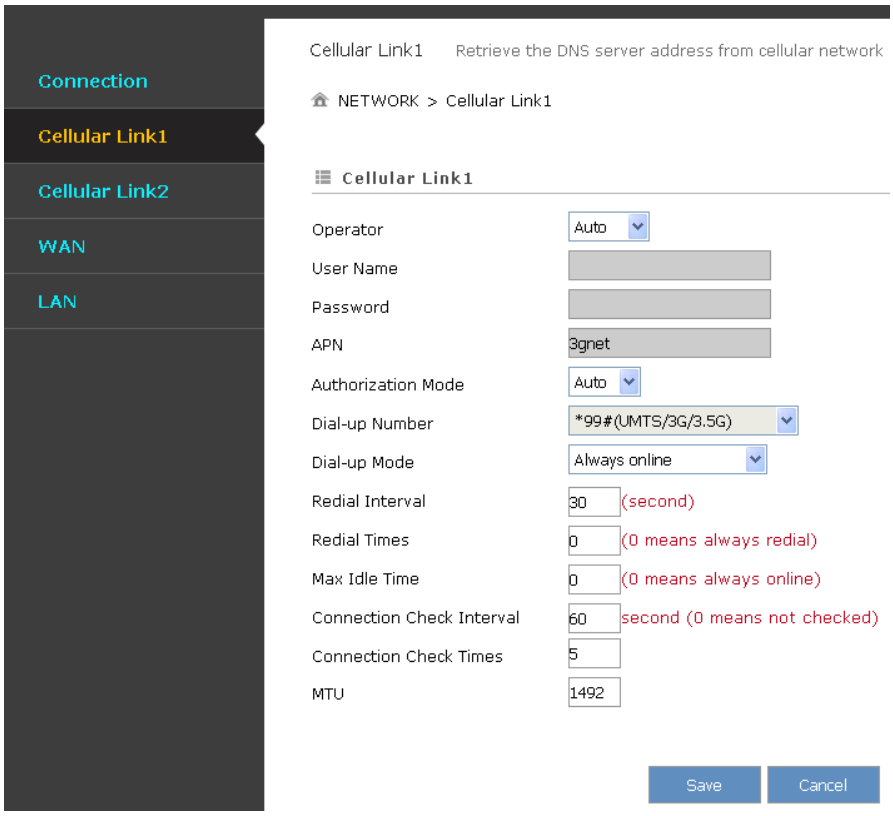
网络拓扑



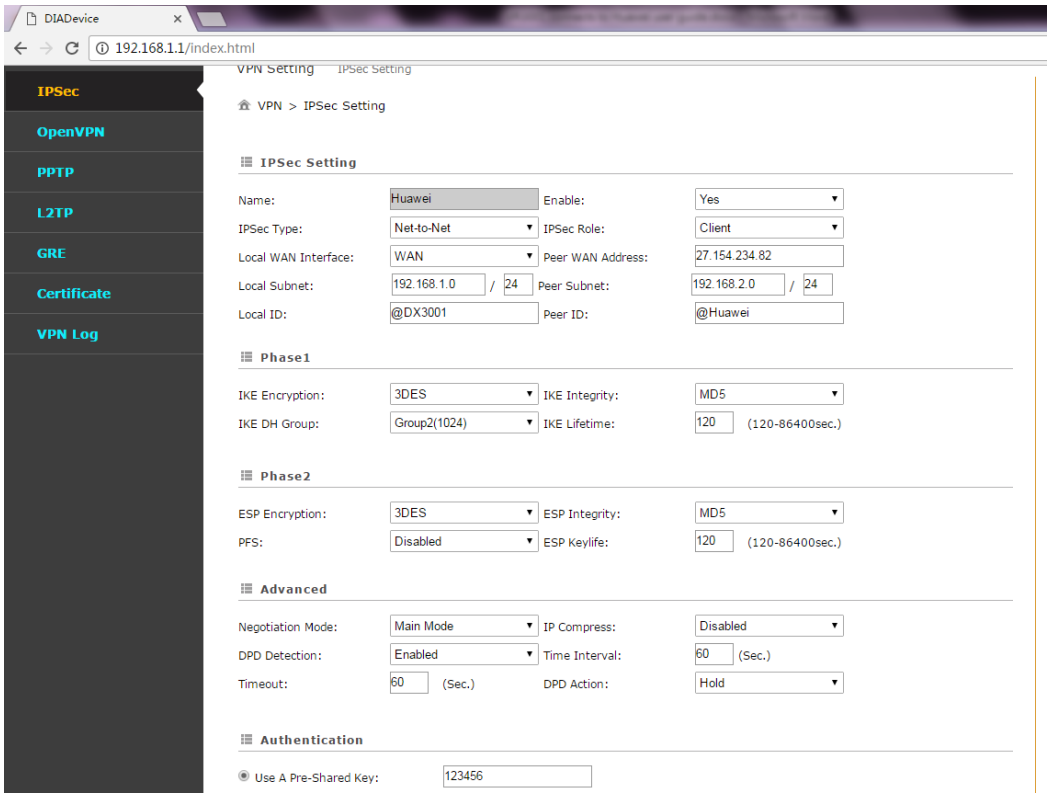
VR301 的设置通过 SIM1 来上网



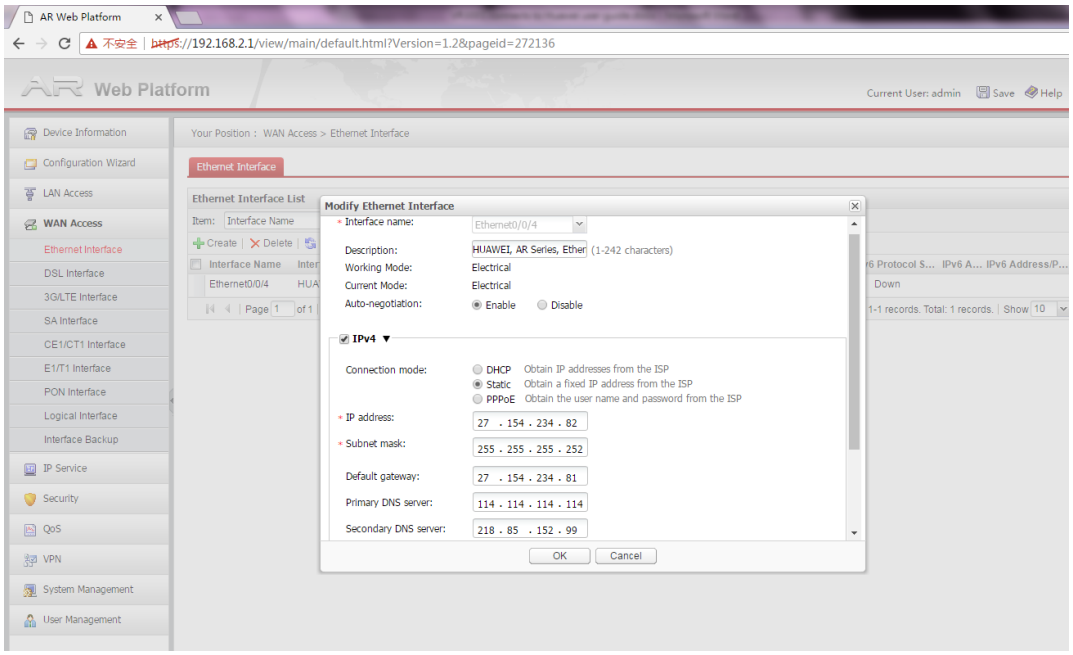
配置 SIM1 的 APN 参数



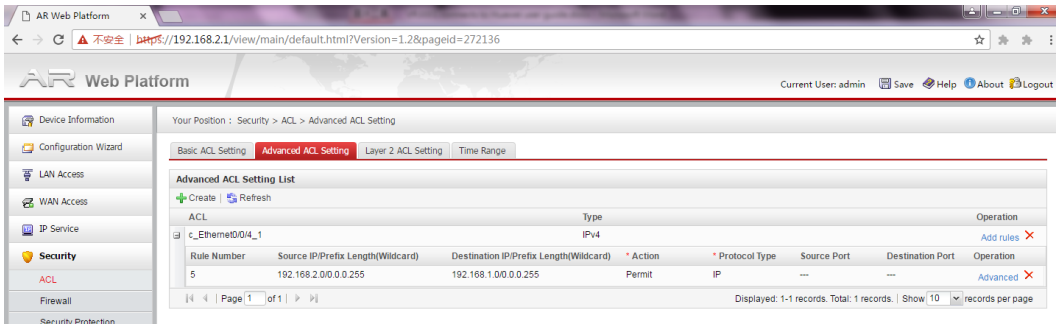
设置 VR301 的 IPSec 参数



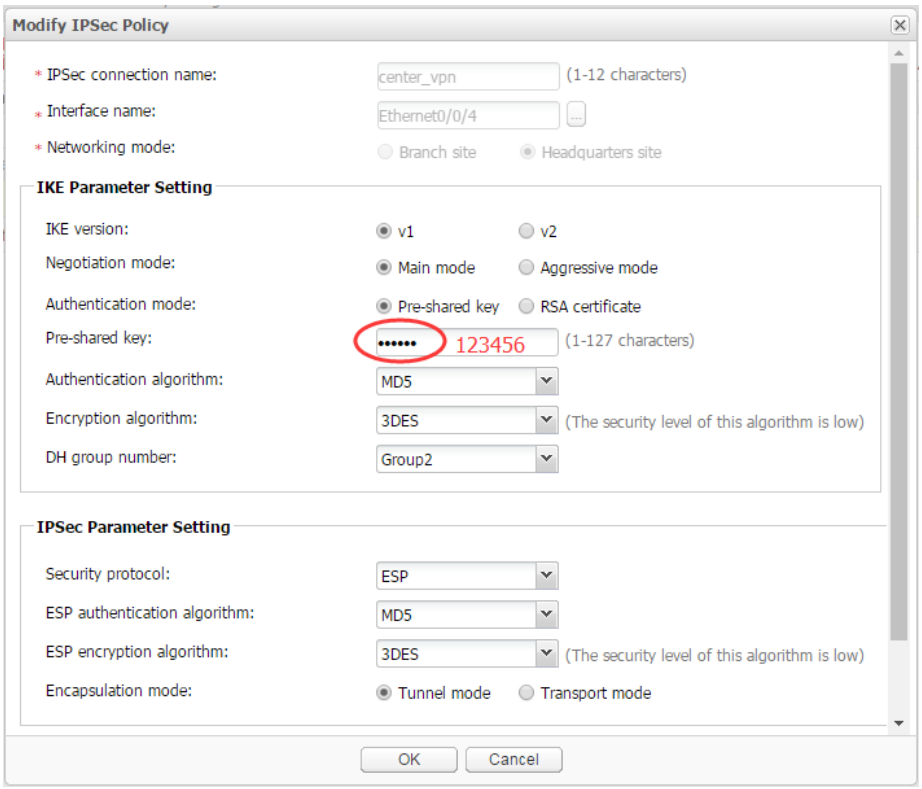
华为的 WAN 口设置



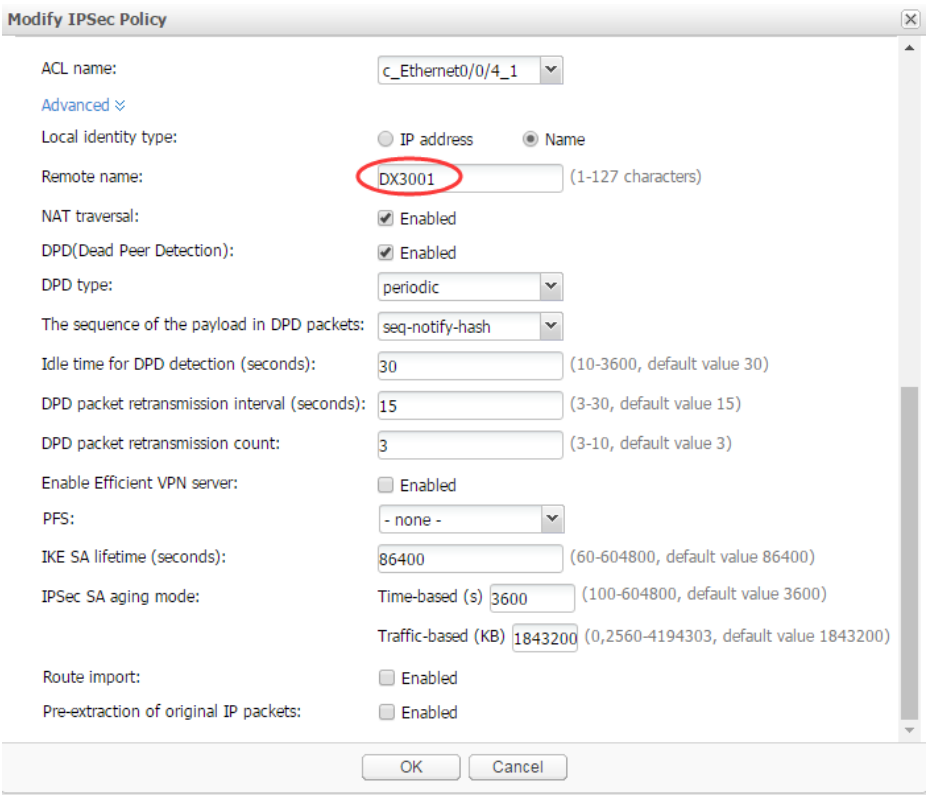
ACL 设置（不然无法通讯）



IPsec 配置截图 1

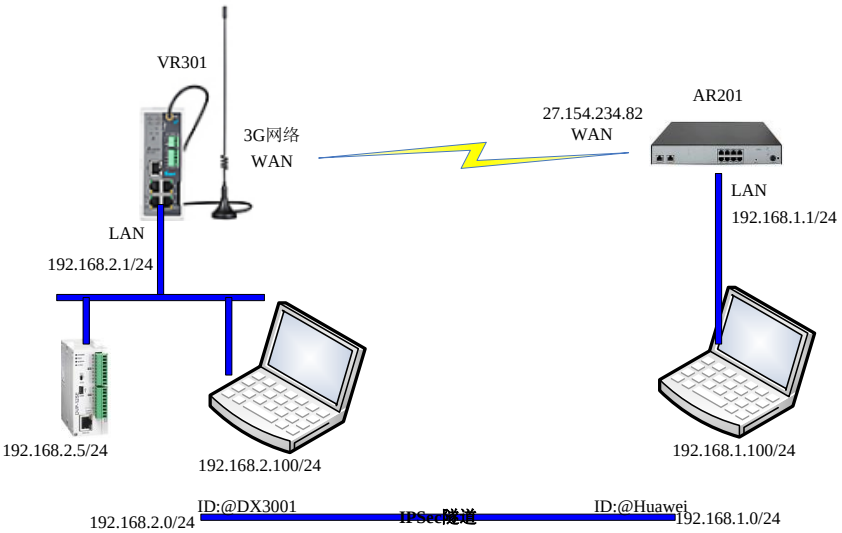


IPsec 配置截图 2

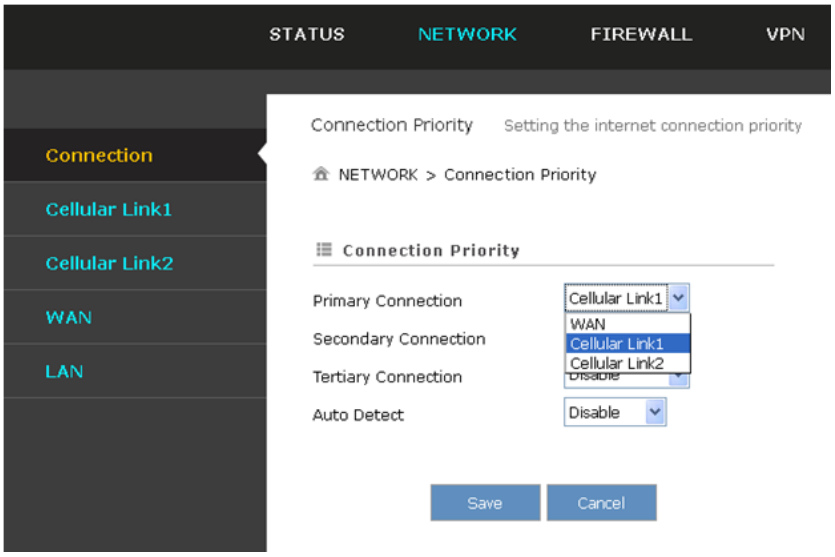


5.1.6 华为 AR201 与 VR301 的 IPsec（PSK）配置

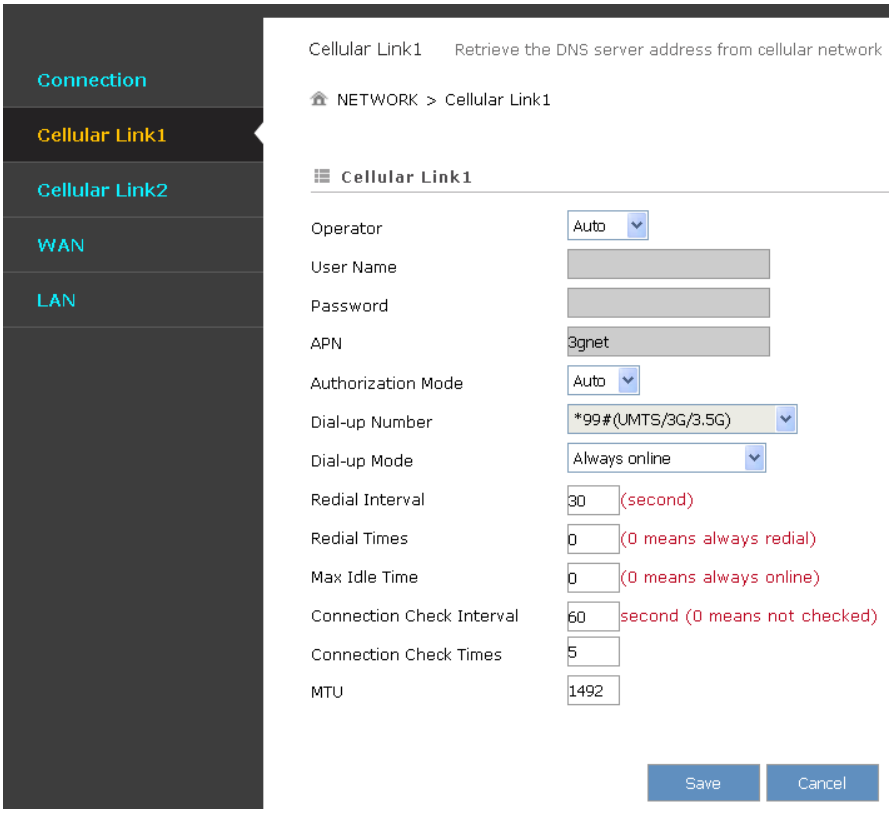
网络拓扑：



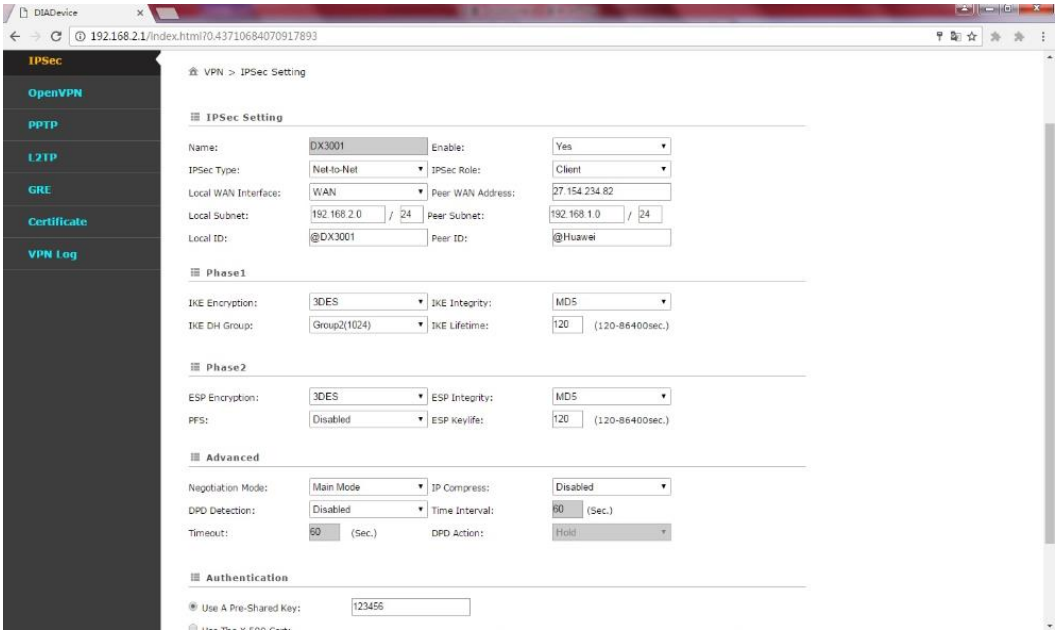
VR301 的设置通过 SIM1 来上网



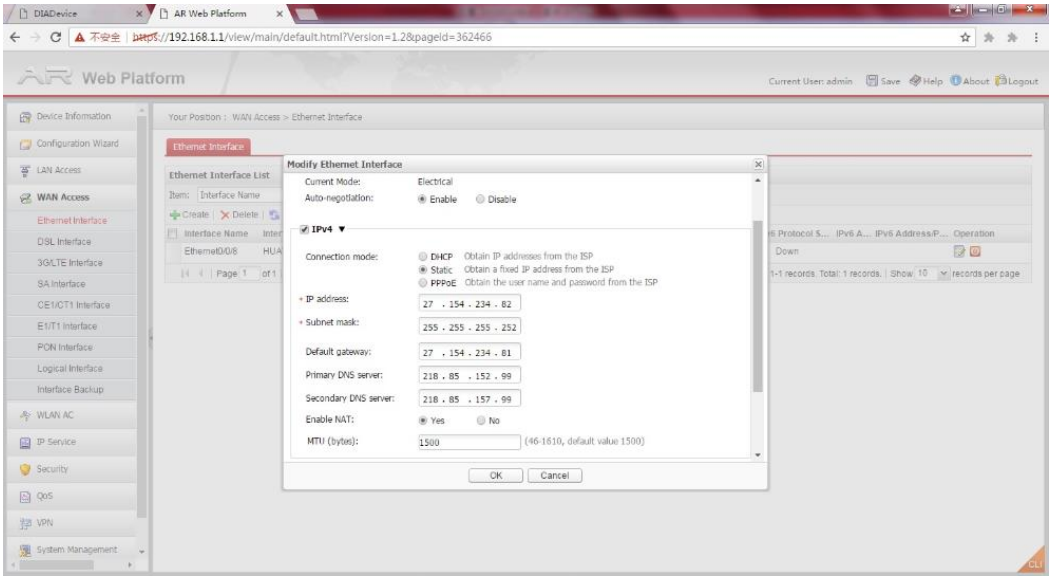
配置 SIM1 的 APN 参数



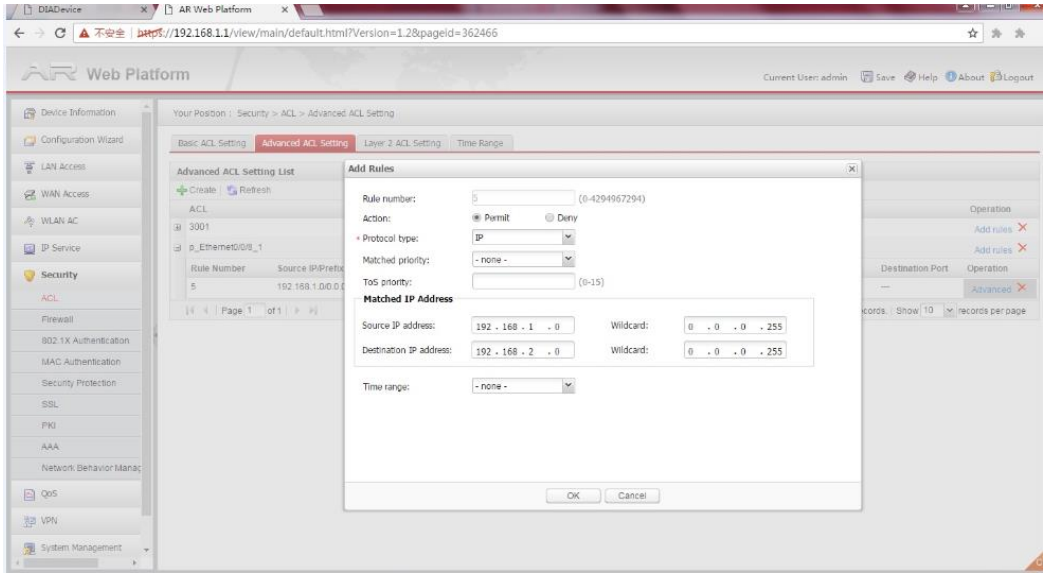
设置 VR301 的 IPSec 参数



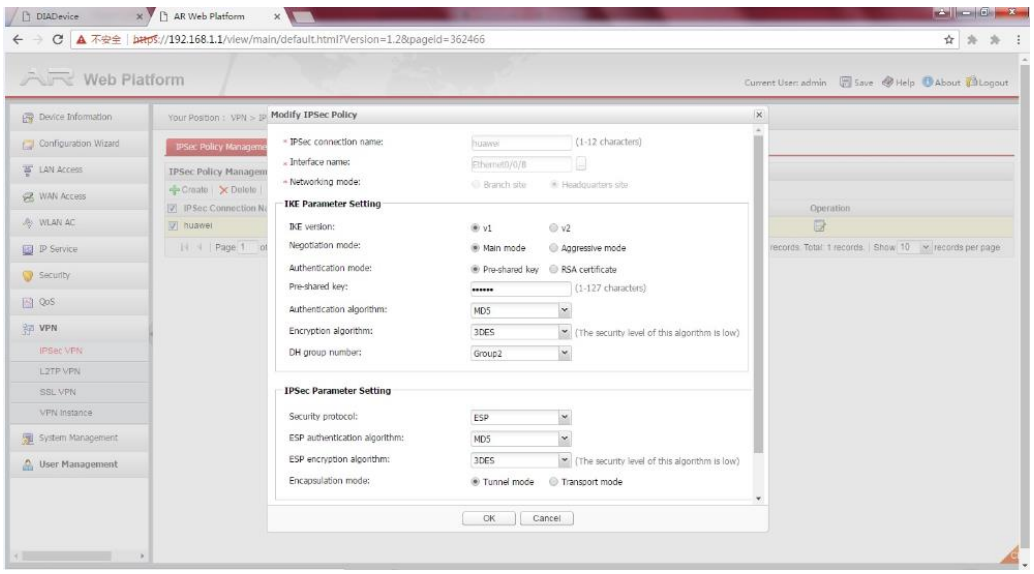
AR201 的 WAN 配置



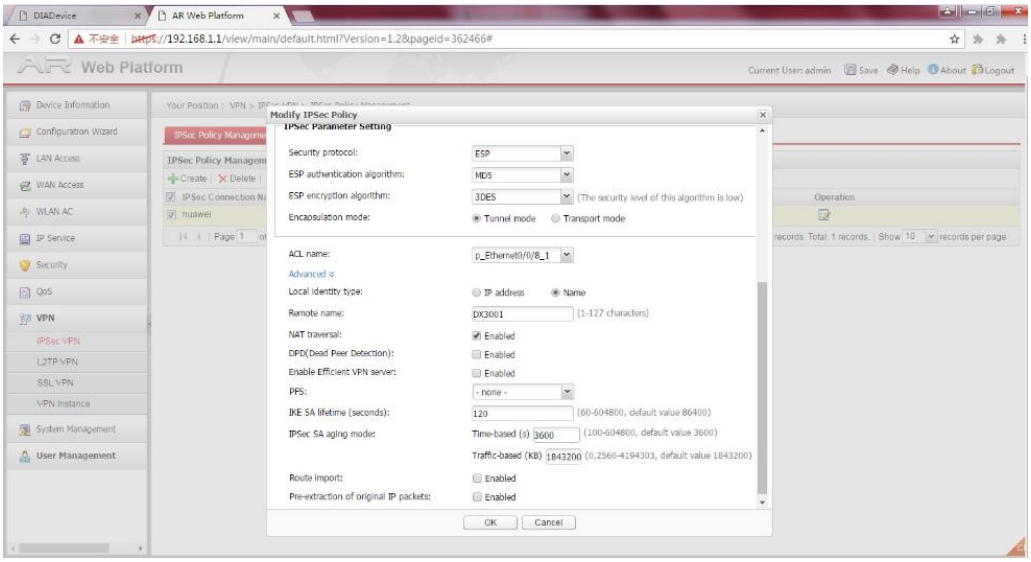
ACL 设置



AR201 的 IPSec 配置 1

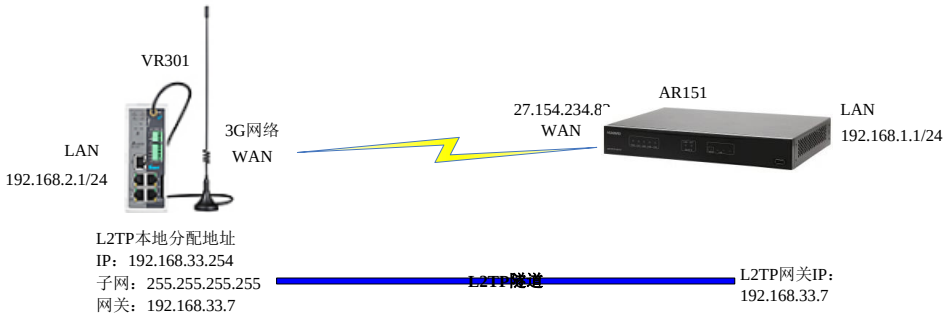


AR201 的 IPSec 配置 2

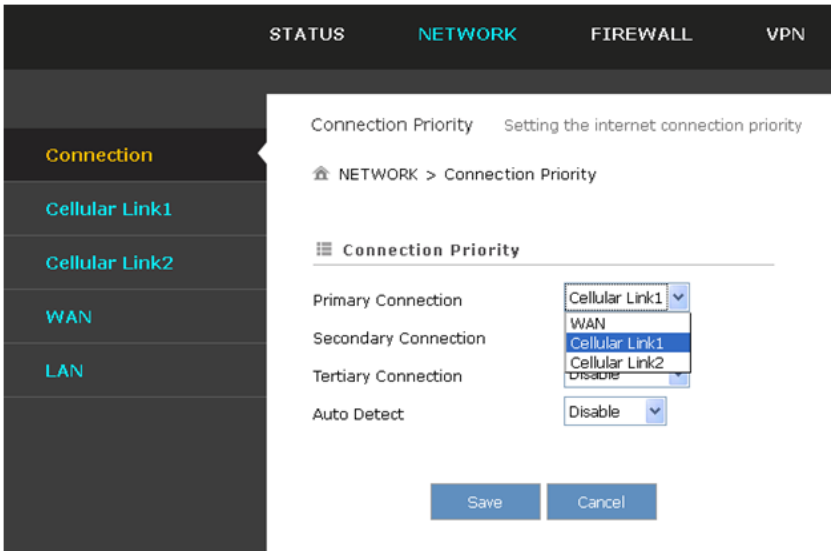


5.1.7 华为 AR151 与 VR301 的 L2TP 配置

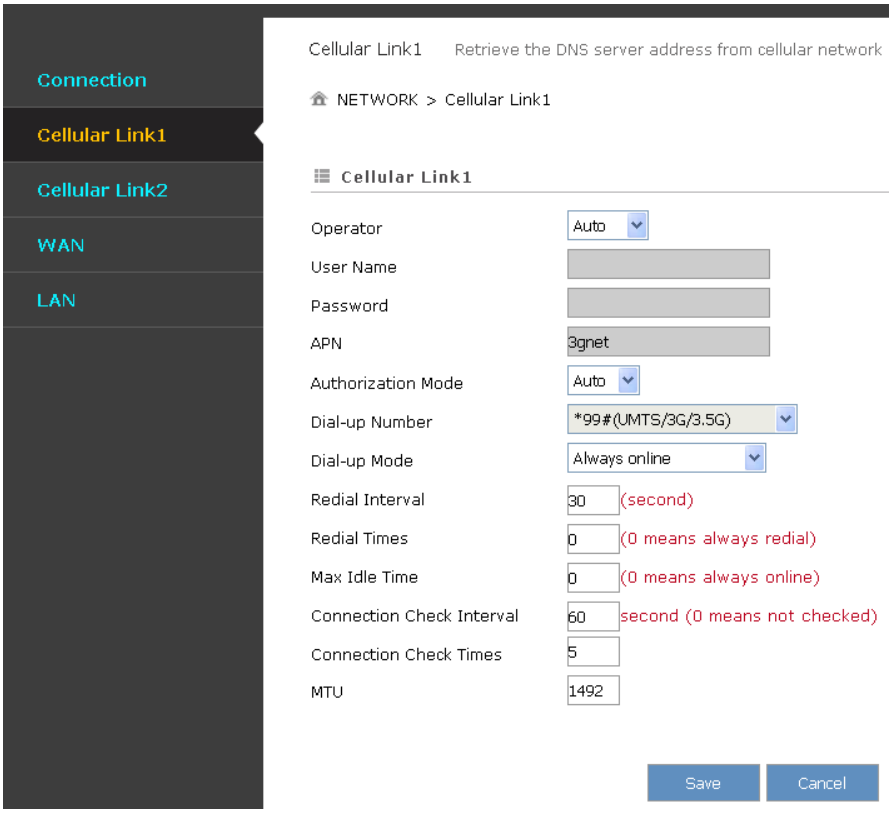
网络拓扑



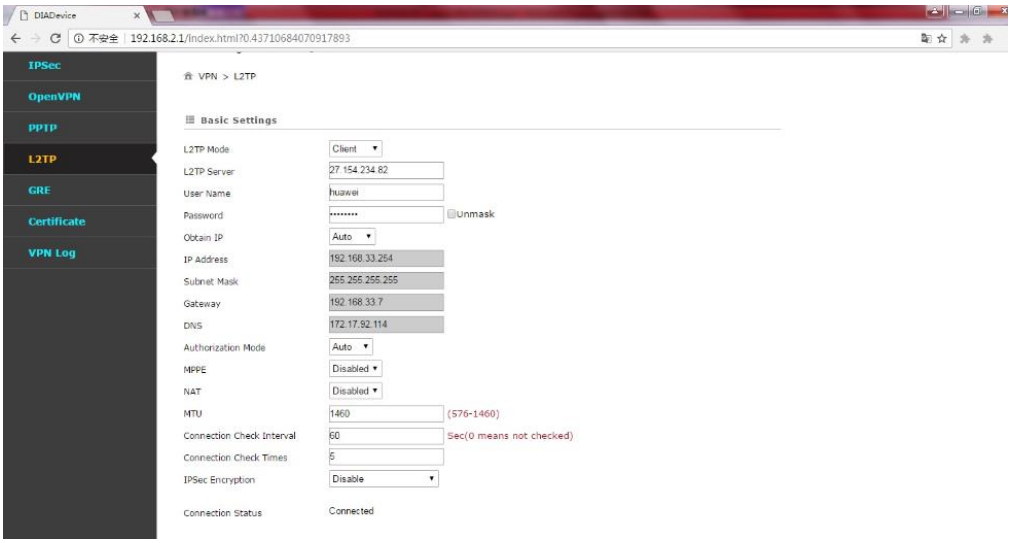
VR301 的设置通过 SIM1 来上网



配置 SIM1 的 APN 参数



VR301 的 L2TP 的配置



AR151 的 WAN 口设置

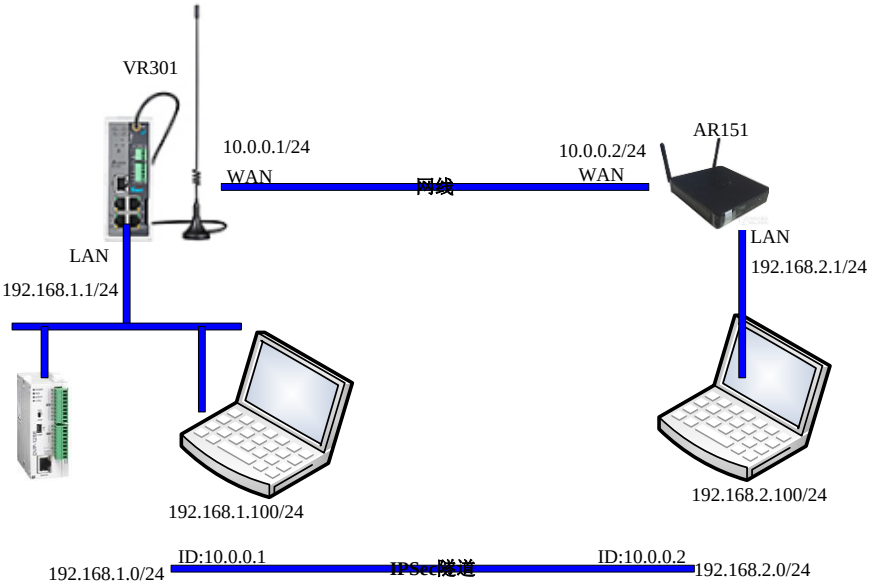
AR151 的 L2TP 配置

AR151 新新建一个用户可以通过 PPP 类型进行接入

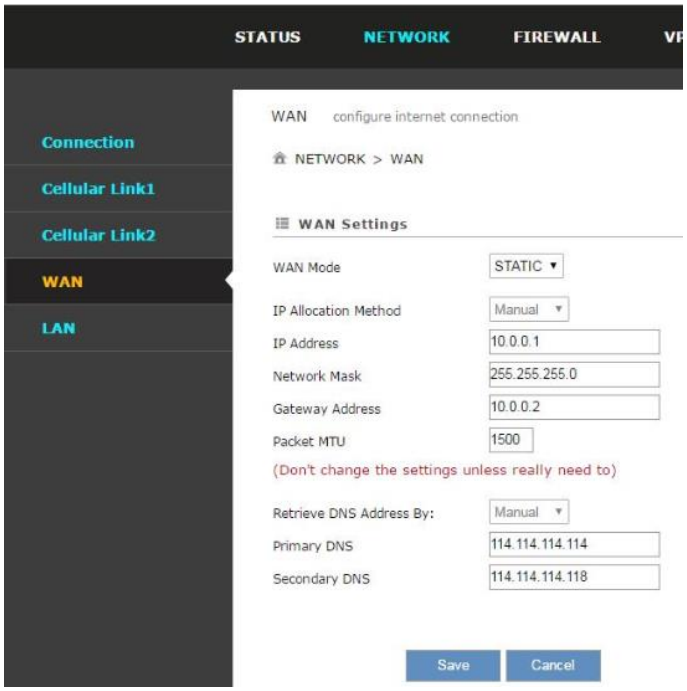
5.2 思科 VPN 路由器与 VR301 的配置

5.2.1 思科 RV130W 与 VR301 的 IPSec（PSK）配置

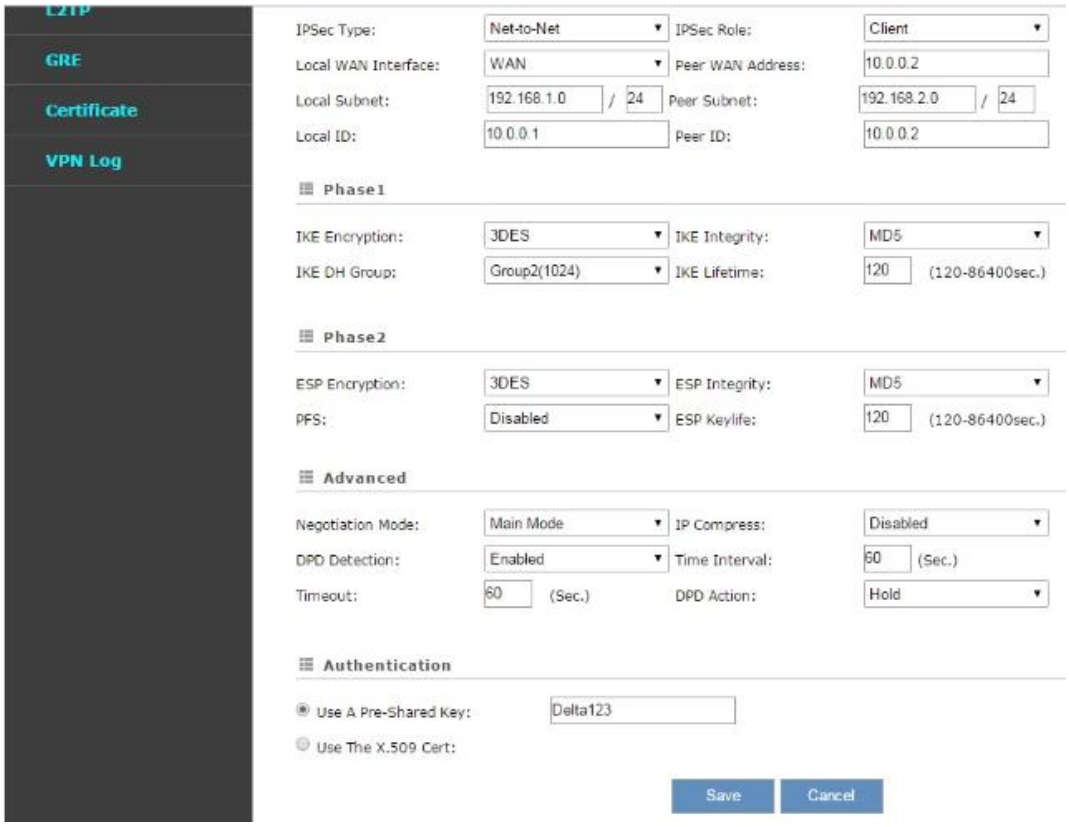
网络拓扑



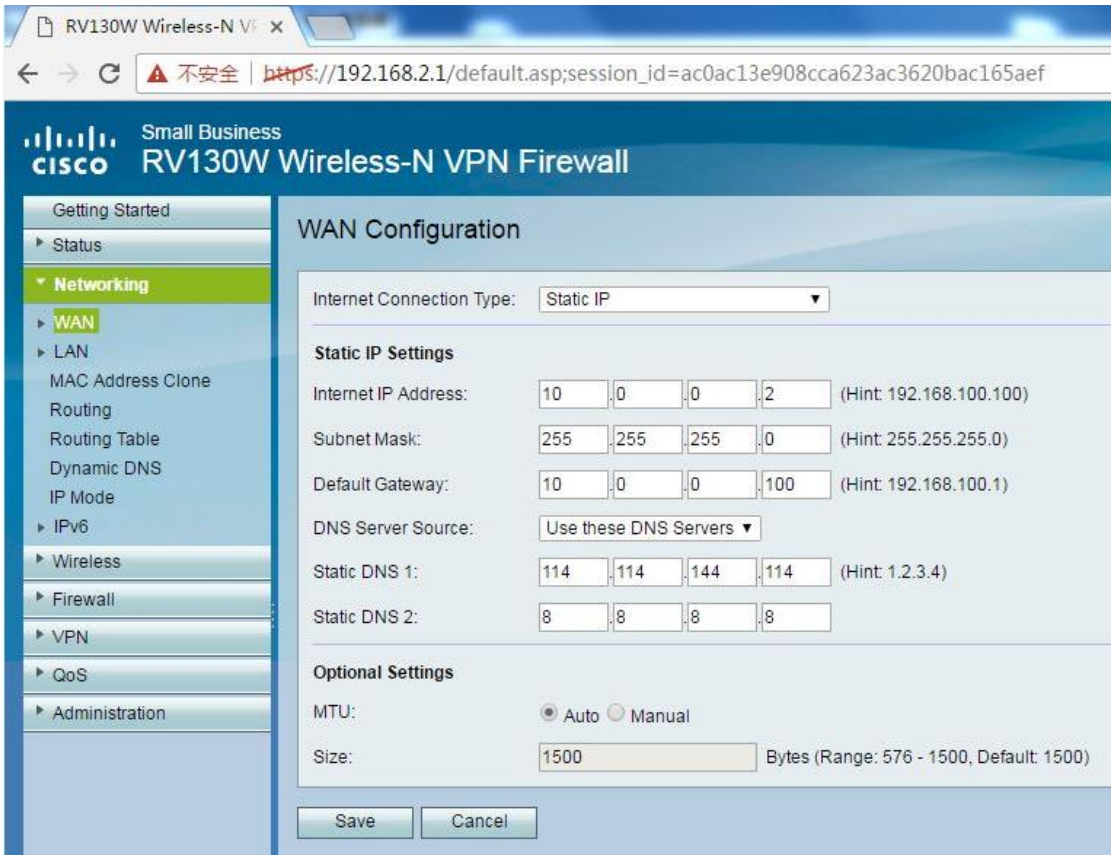
VR301 的 WAN 口配置



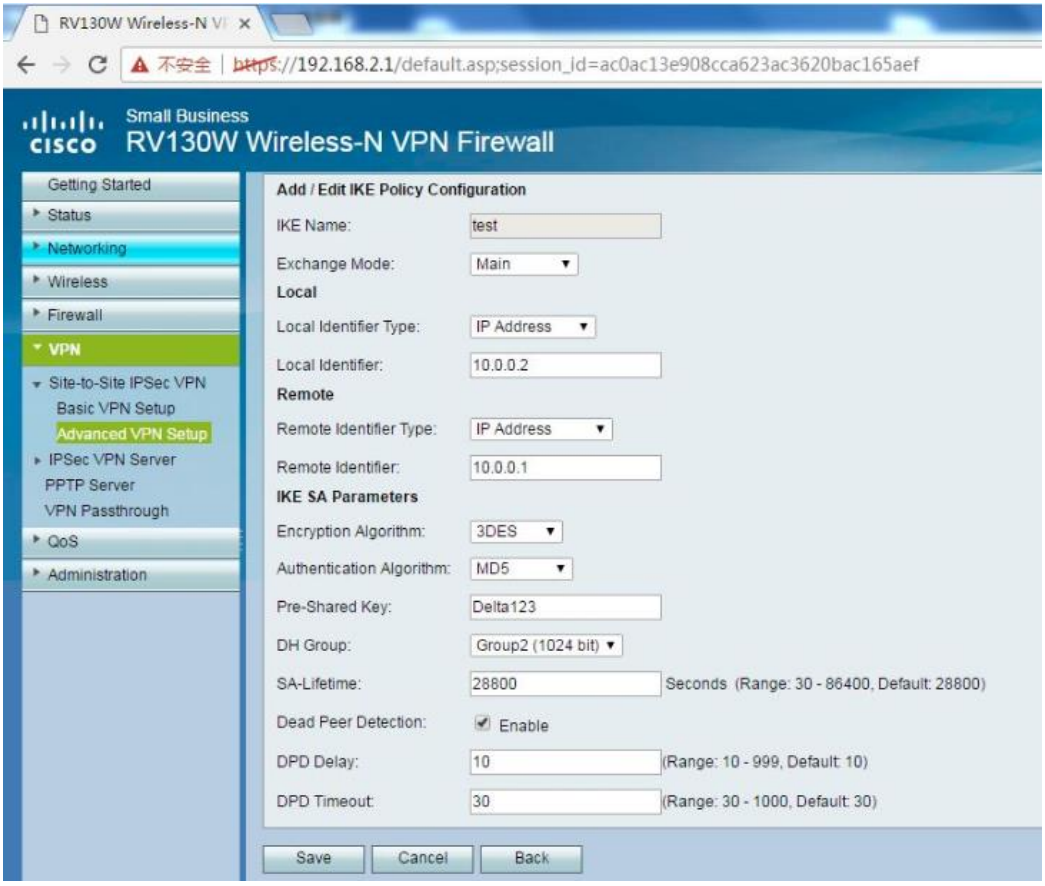
VR301 的 IPSec 配置



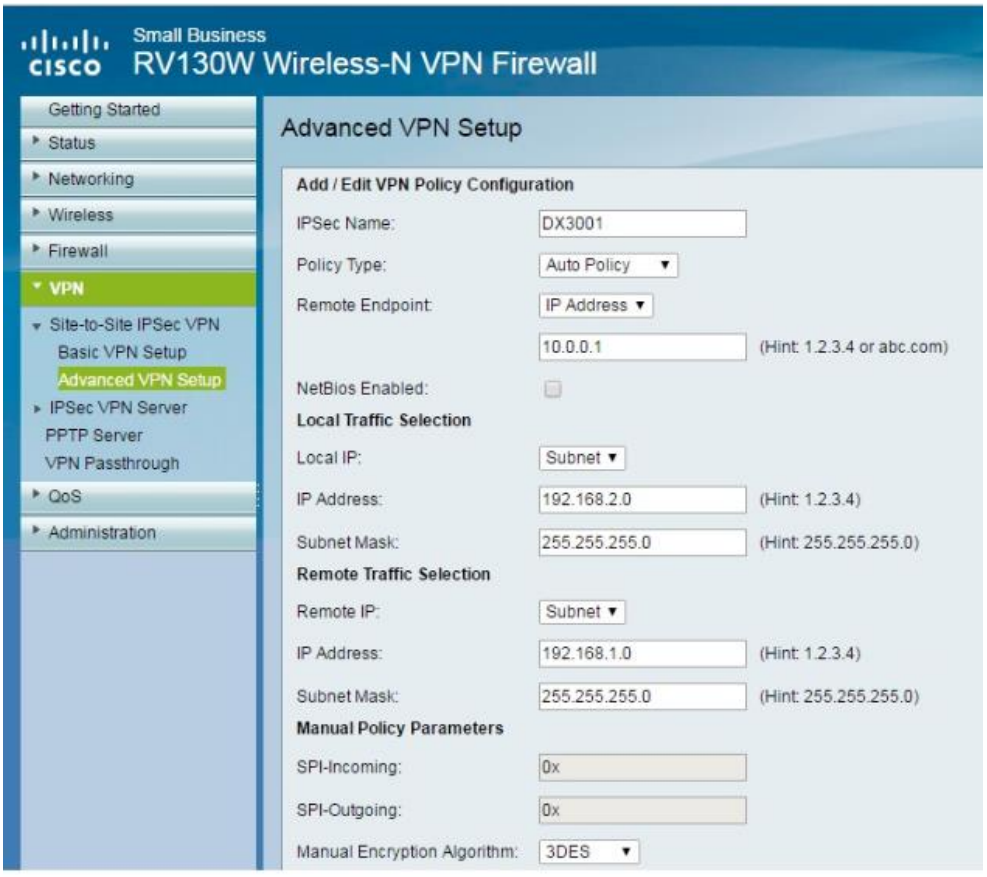
思科 RV130W 的 WAN 口配置



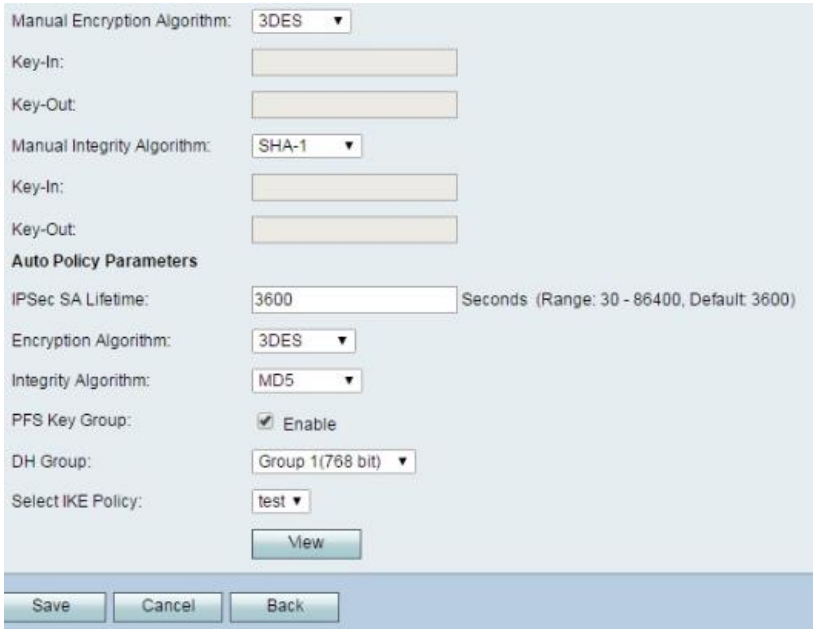
思科 RV130W 的 IPSec 配置 1



思科 RV130W 的 IPSec 配置截图 2

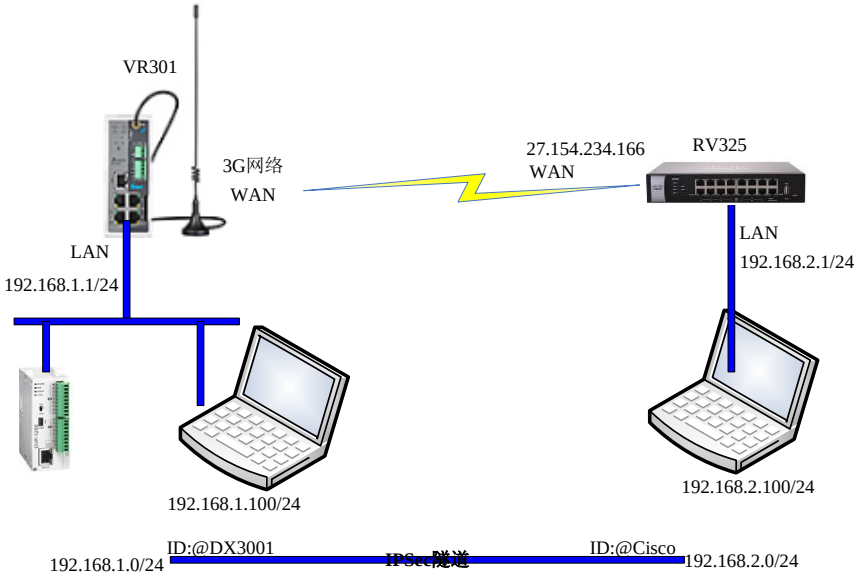


思科 RV130W 的 IPSec 配置截图 3

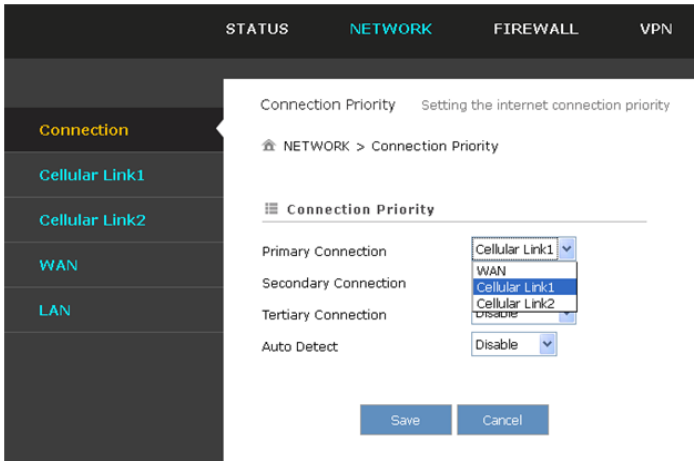


5.2.2 思科 RV325 与 VR301 的 IPSec（PSK）配置

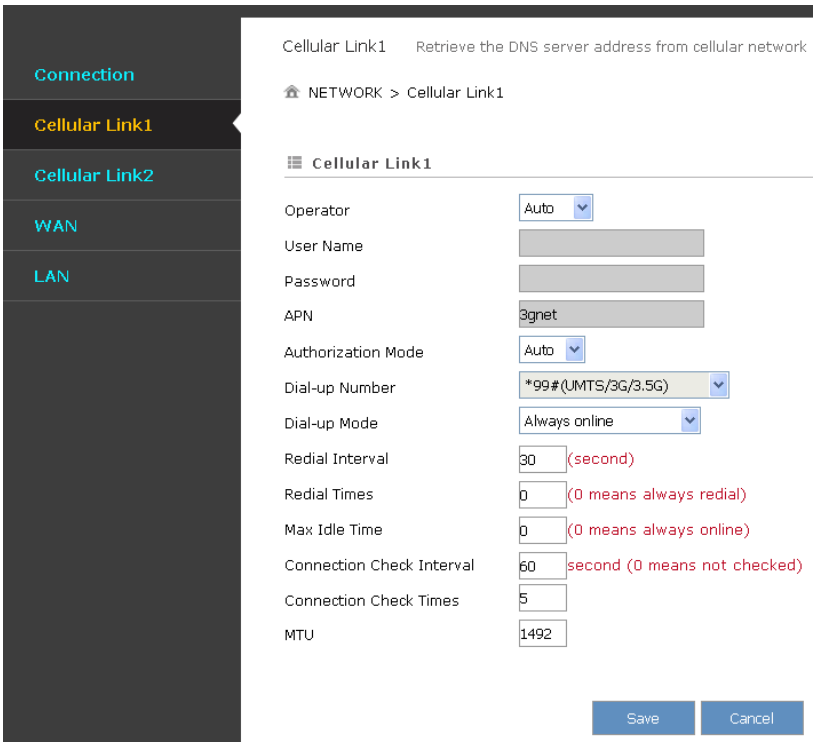
网络拓扑



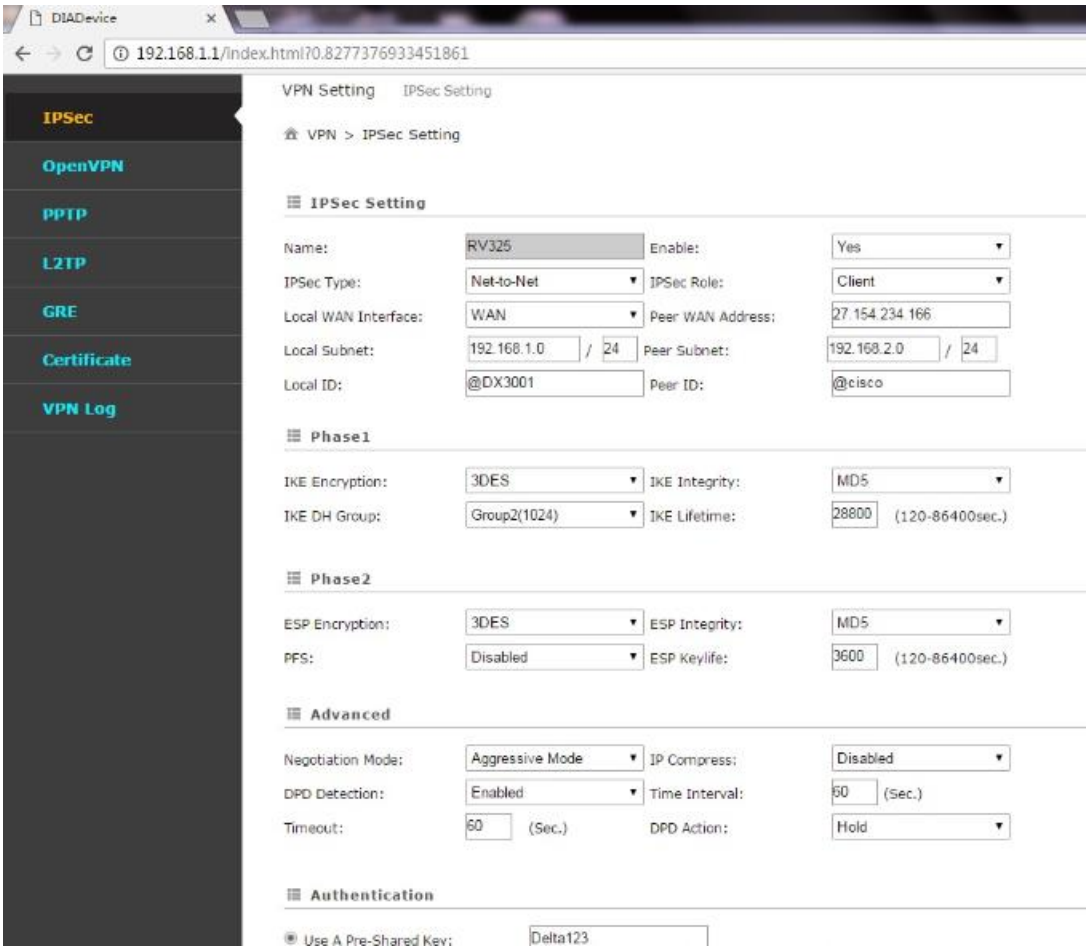
VR301 的设置通过 SIM1 来上网



配置 SIM1 的 APN 参数

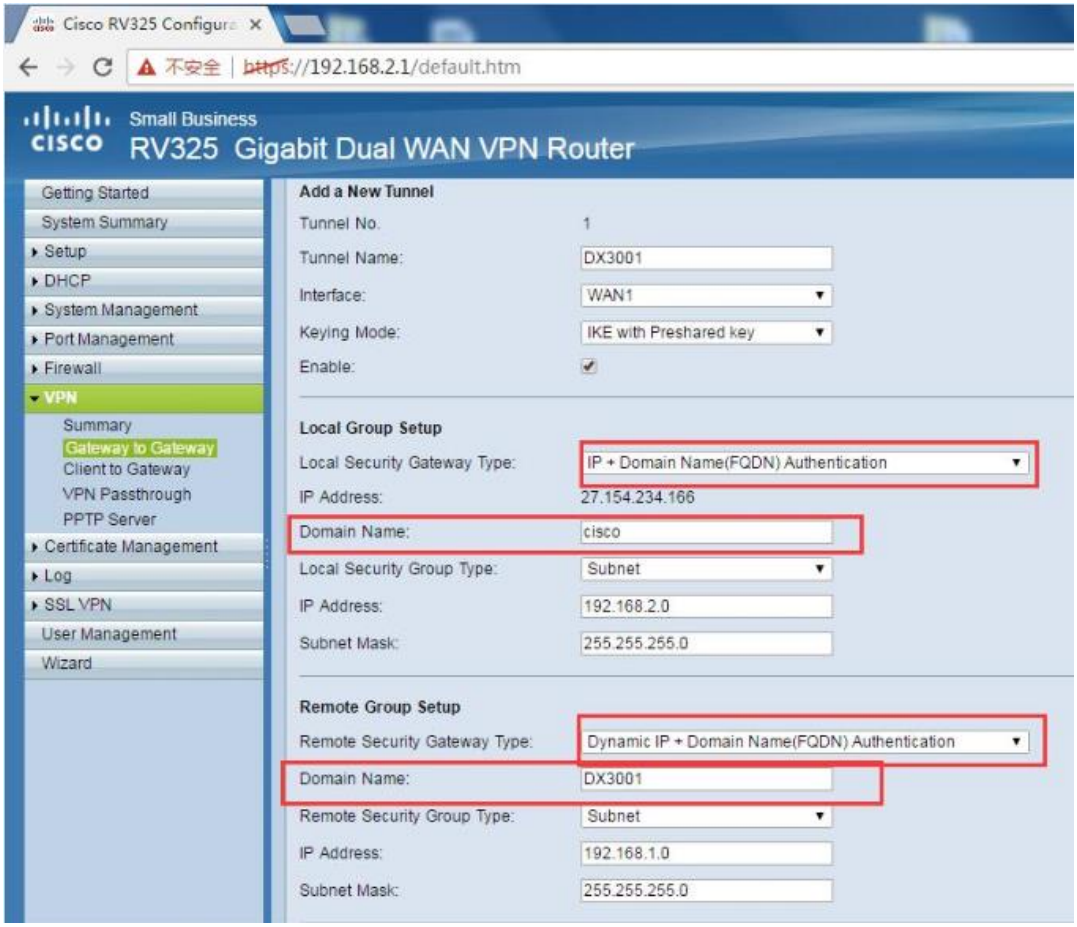


VR301 的 IPSec 配置

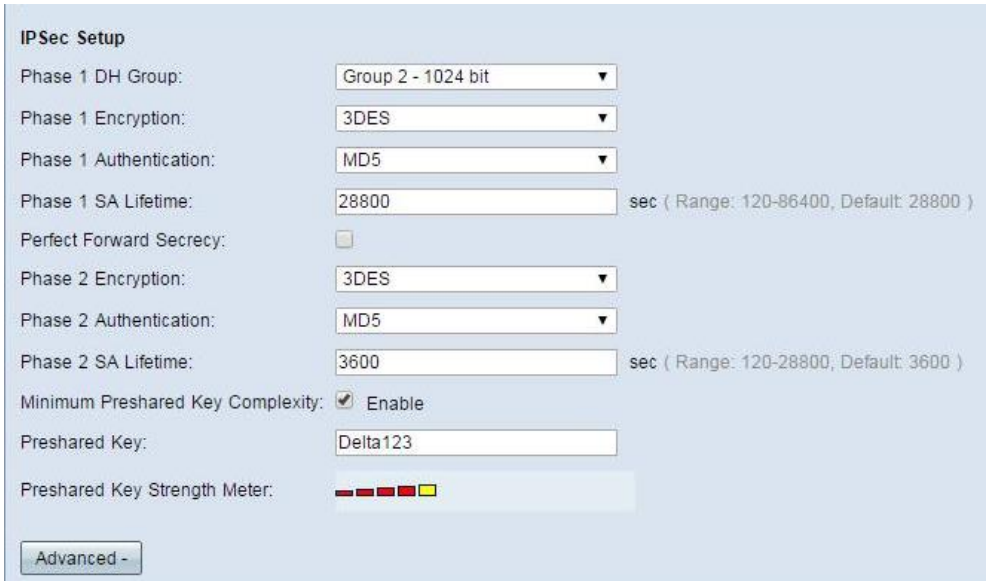


RV235 的 WAN 口配置

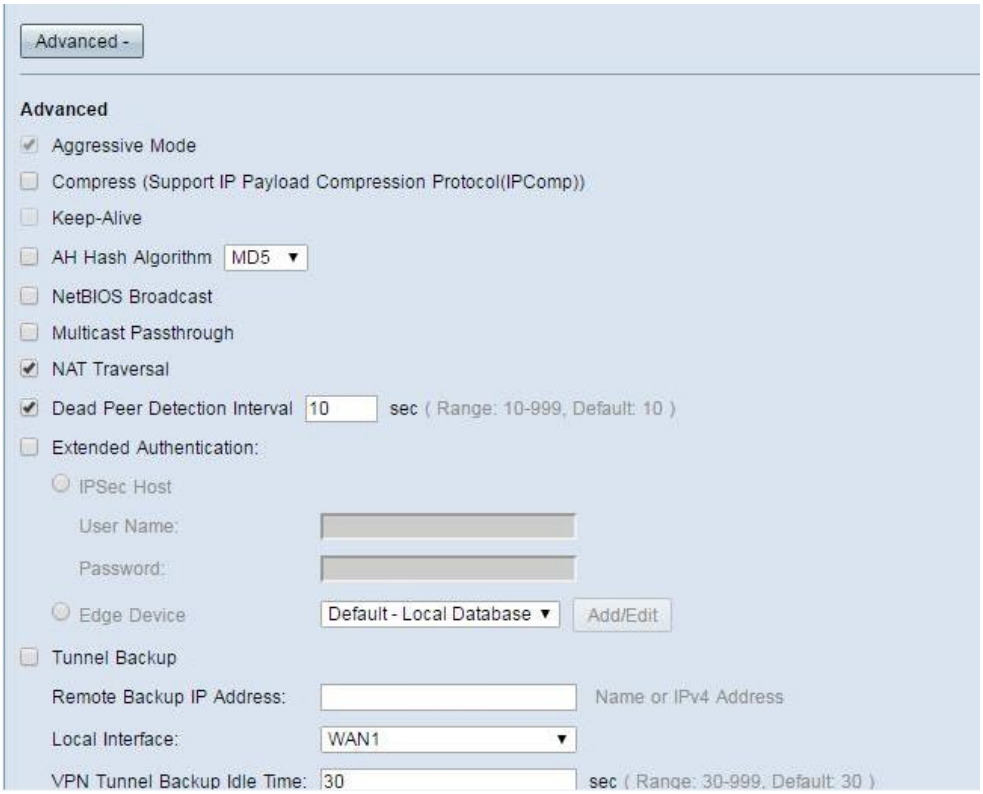
RV235 的 IPSec 配置截图 1



RV235 的 IPSec 配置截图 2



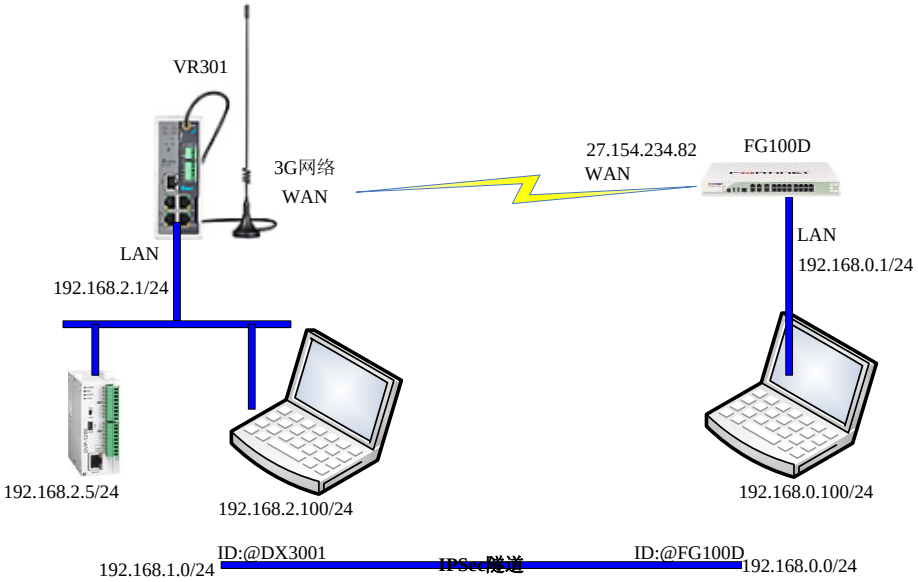
RV235 的 IPSec 配置截图 3



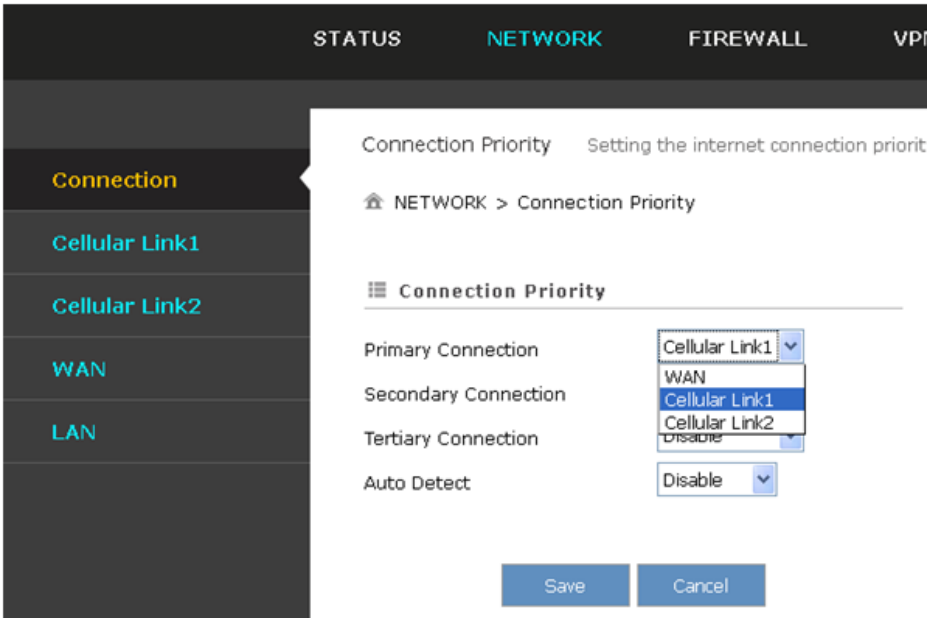
5.3 飞塔 Fortinet

5.3.1 飞塔 FG100D 与 VR301 的 IPsec（带证书）的配置

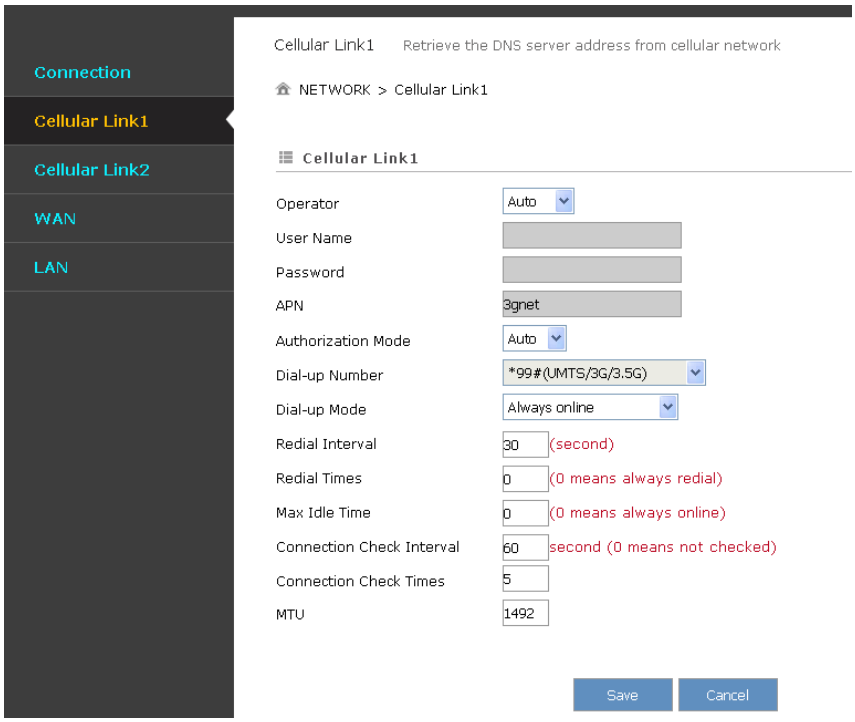
网络拓扑



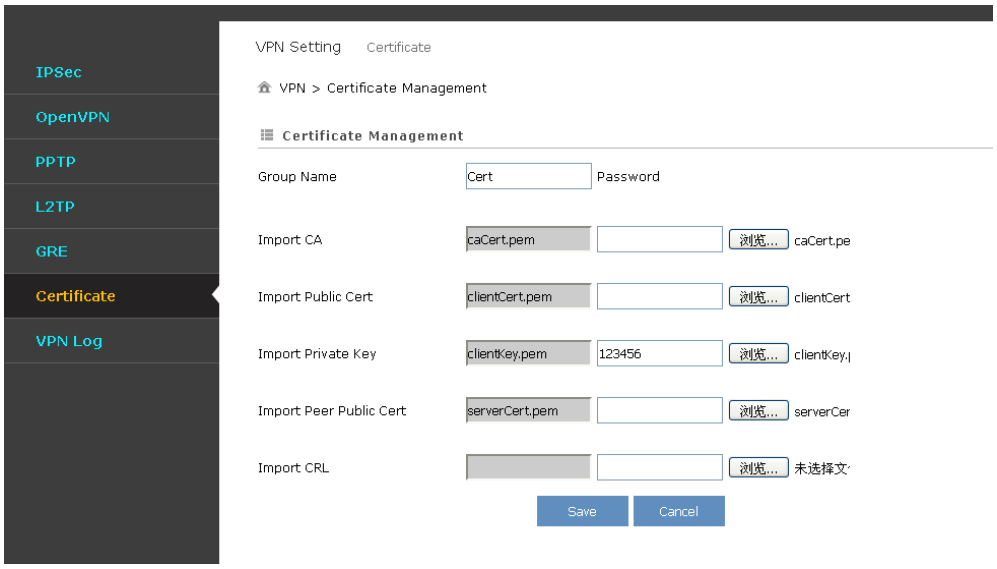
VR301 的 SIM1 的配置



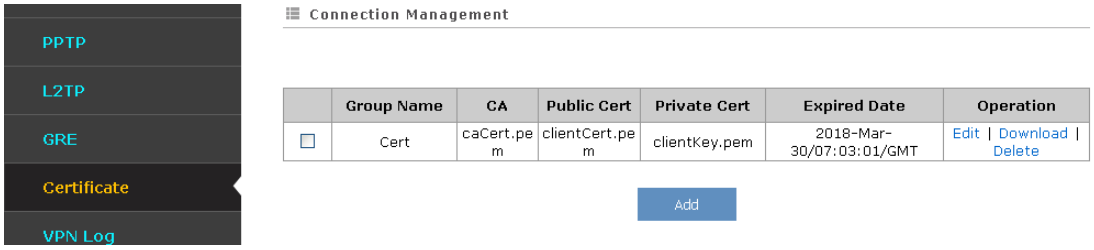
VR301 的 SIM1 的 APN 参数设置



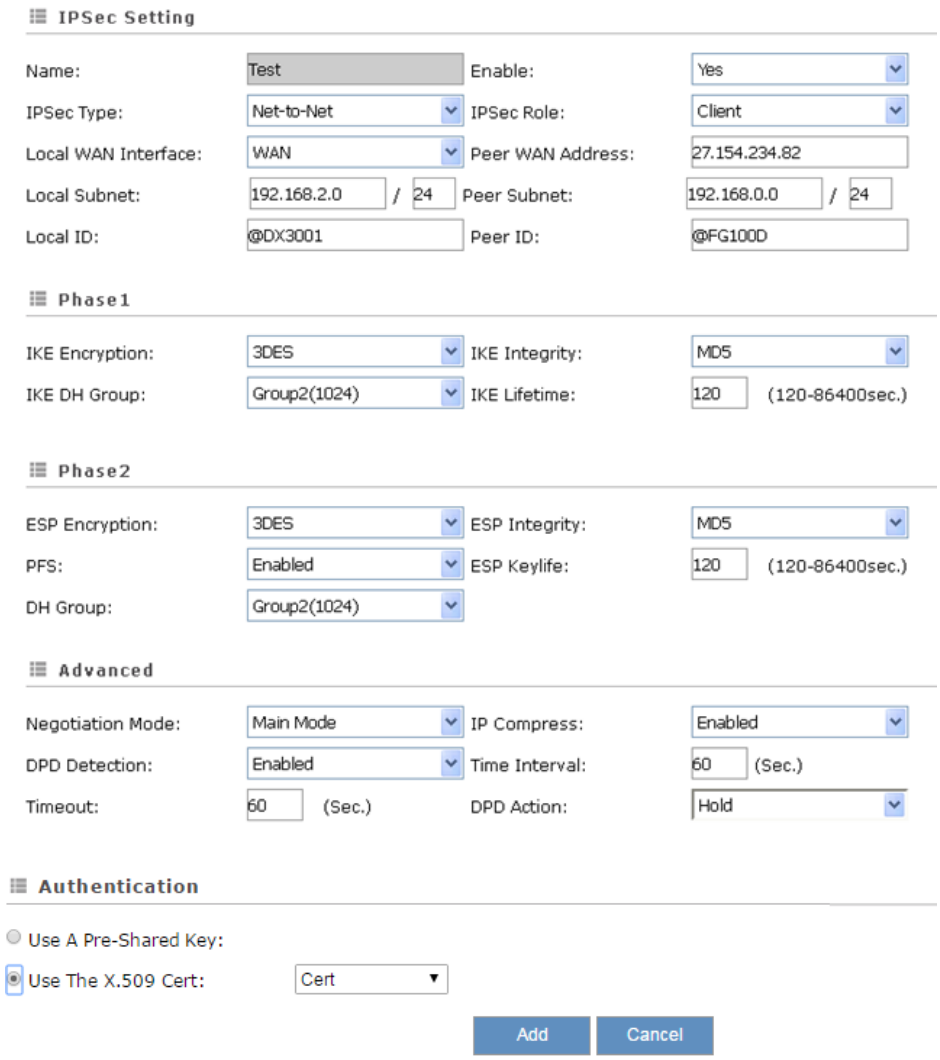
VR301 的 VPN 证书导入



导入后显示如下：



VR301 的的 IPSec 配置



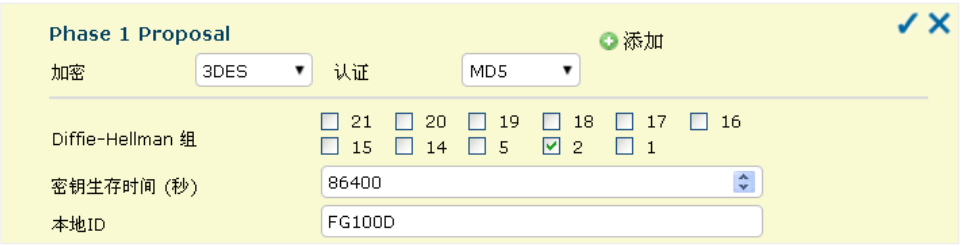
FG100D 的 WAN 口配置

FG100D 的 IPSec 配置截图 1

FG100D 的 IPSec 配置截图 1

FG100D 的 IPSec 配置截图 2

FG100D 的 IPSec 配置截图 3



FG100D 的 IPSec 配置截图 4

6 福达 VPN 模块应用案例

6.1 供水供水公司远程监控

6.1.1 背景

水厂自动控制系统适用于供水企业远程控制管理水厂，水厂操作人员可以在水厂控制室远程监测厂内水池水位、进厂流量、出厂流量、出厂压力、水质等信息；远程监测加压泵组、配电设备及其它自动化设备的工作情况；可以远程控制加压泵的启停等操作。

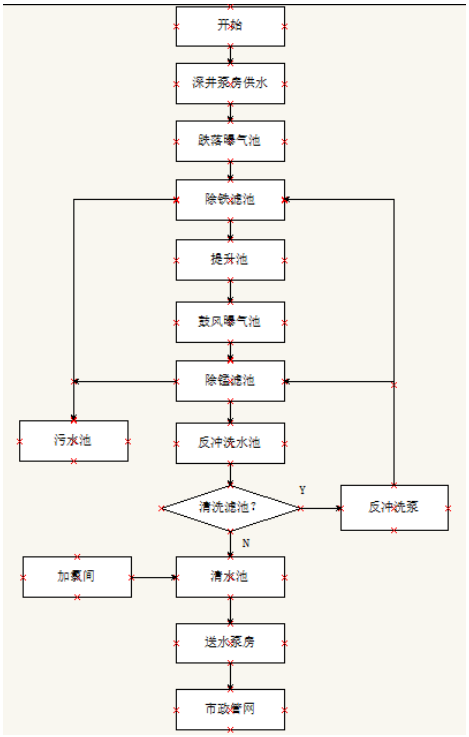
6.1.2 方案概述

工艺简介

该水厂采用的水源为深井地下水，故其水处理工艺流程较简单，主要包括以下几个流程：

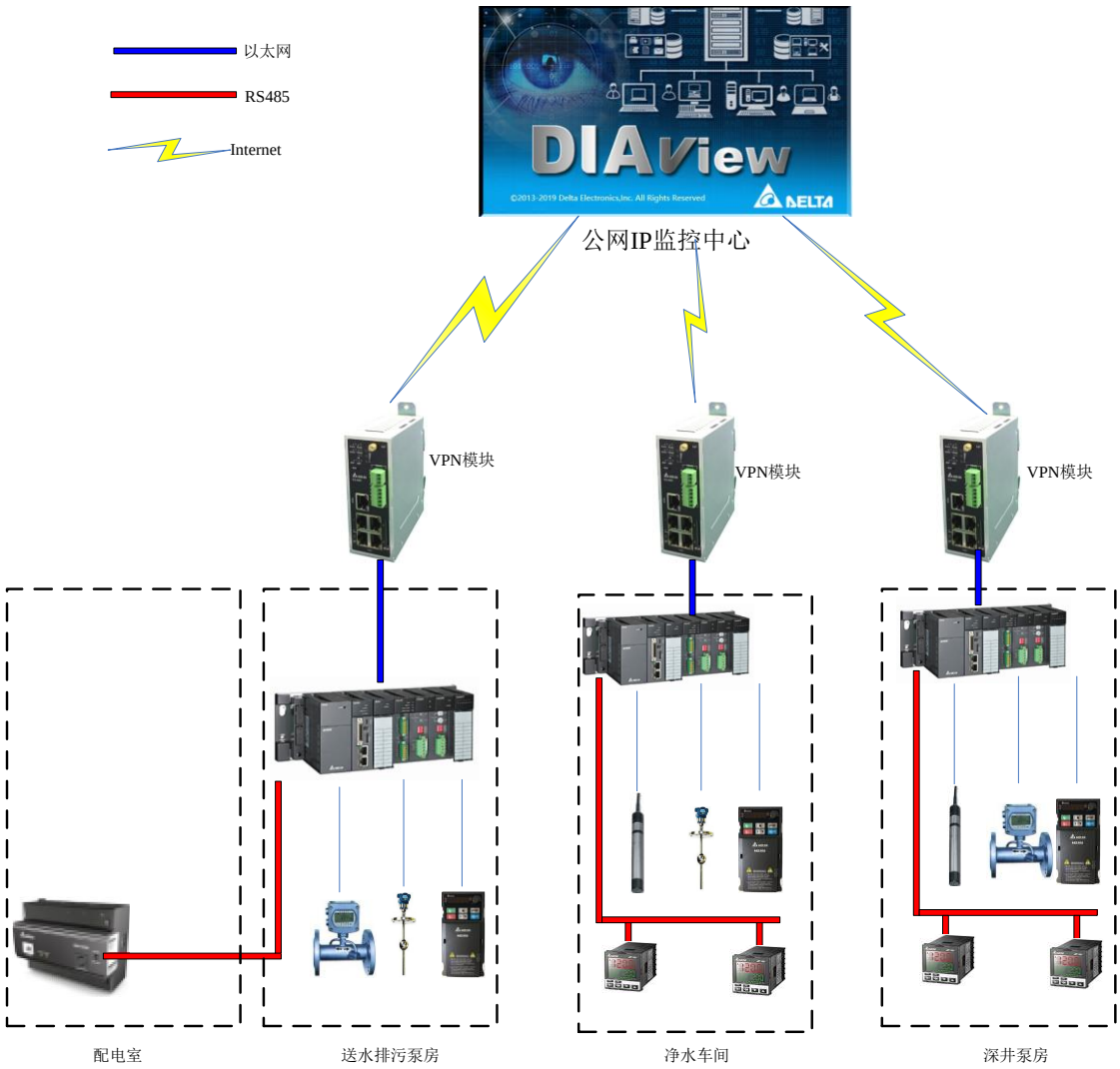
1. 跌落曝气：将地下水直接抽取上来采取自然跌落的方式让地下水的含氧量达到 4%-5%左右，以便后续的工艺流程。
2. 除铁：通过滤料将水中的铁原素去除。
3. 鼓风曝气：将除铁后的的水提升到鼓风曝气池，采用鼓风机向池内强制打氧，将水的含氧量提高，以便后续的工艺流程。
4. 除锰：通过相应的滤料将水中的锰原素去除。
5. 加氯：将去除锰原素的水加氯消毒。

具体的工艺流程如下图：



组网方案

监控中心向运营商购买公网 IP，各个站点通过 VPN 模块连接成 VPN 专网。监控中心通过 DIAView 去连各个站点的 PLC。

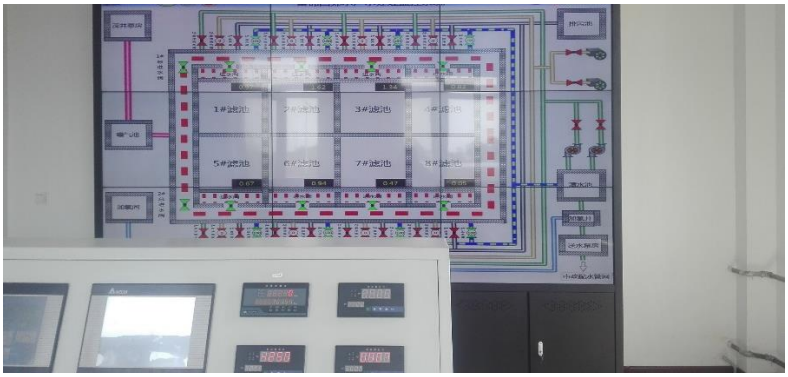


电气清单

名称	型号	数量	说明
PLC	AHCPU510-RS2	1	送水、排污泵房
	AHCPU520-EN	1	净水车间
变频器	VFD750CP43B-00	4	送水泵
	VFD220CP43B-21	2	排污水
	VFD055CP43B-21	2	排污泥
	VFD370CP43B-21	7	深井泵
	VFD300CP43B-21	3	提升泵
HMI	DOP-B10S411	1	深井泵
	DOP-B10E615	1	净水车间
组态软件	DIAView	1	监控中心
电力仪表	DPM-C520I	1	配电室
VPN 模块	VR101L1	3	每个现场一台

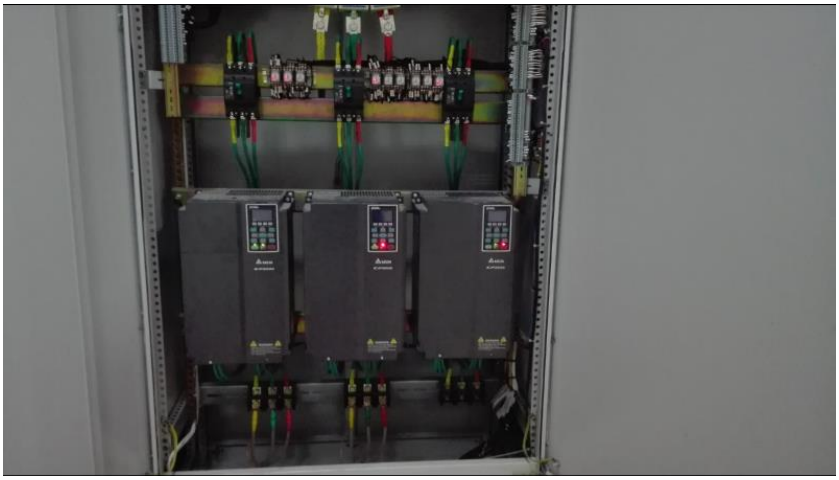
6.1.3 现场图片

监控中心站点照片



净水间电控柜

提升泵的变频柜



6.2 包装生产线的 VPN 联网方案

6.2.1 背景

XX 包装公司，有多个分厂，由于数据没有集中导致监控管理困难。而产线又面临多种多样的困难。

（1） 所有改造不能干扰正常生产

（2） 目前所有产线的 IP 可能相同，也可能不在同一个网段

（3） 现场网络部分有网线，部分地方网线没法布线

（4） 工厂较为分散，国内四个工厂在不同省份，还有两个工厂在国外

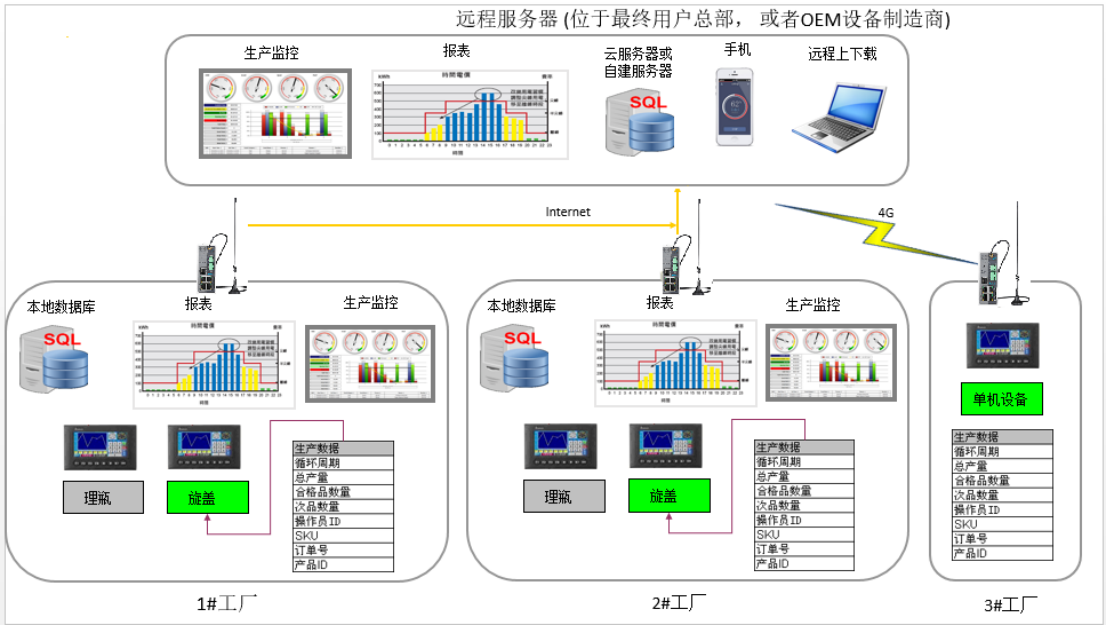
（5） 工厂的所有数据不能托管在第三方平台

（6） 所有数据传输都需要进行加密

为了解决上述的种种困难，采用了福达的 VPN 组网方案。

6.2.2 组网方案

监控中心向运营商购买公网 IP，各个站点通过 VPN 模块连接成 VPN 专网。



6.2.3 方案优势

（1）福达 VPN 模块内置防火墙功能，完美规避了现场 IP 冲突所带来的问题；

（2）VPN 模块均有双 SIM 卡和有线的网络冗余，最大限度的规避了 VPN 模块断网的情况；

（3）VPN 模块丰富的网络接入，给现场设备选型和布线带来了极大的方便
（4）VPN 采用多种加密方式，使得数据传输更加安全；
（5）VPN 组网后，相当于虚拟的局域网。原有的局域网监控技术可以实现平滑过渡；
（6）VPN 组网，可以动态的增删监控站点，未来的扩展更加方便。