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: <u>sales@vidagrid.com</u>
- 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。



© DELTA NETWORKS (XIAMEN) LTD.

All rights reserved

目录

用一草 产品介绍	6
1.1 产品概览	6
1.2 选型	6
1.3 外观及其安装尺寸	7
1.3.1 正面面板及其指示灯	8
1.3.2 顶部平面	8
1.3.3 底部平面	9
1.3.4 安装尺寸	9
第二章 WEB 配置页面访问	10
2.1 连线	10
2.2 默认 IP 和登陆账号及密码	10
2.3 更改电脑 IP	10
2.4 登陆	13
第三章 功能说明	15
3.1 状态	15
3.1.1 网络状态	15
3.1.2 设备信息	15
3.1.3 日志	
3.2 网络设置	
3.2 网络设置 <i>3.2.1 连接优先级配置</i>	
 3.2 网络设置 3.2.1 连接优先级配置 3.2.2 SIM 卡1 设置 	
 3.2 网络设置 3.2.1 连接优先级配置 3.2.2 SIM 卡1 设置 3.2.3 SIM 卡2 设置 	
 3.2 网络设置 3.2.1 连接优先级配置 3.2.2 SIM 卡1 设置 3.2.3 SIM 卡2 设置 3.2.4 WAN 设置 	
 3.2 网络设置 3.2.1 连接优先级配置	
 3.2 网络设置	
 3.2 网络设置	
 3.2 网络设置	

3	3.3.4	Port Trigger 设置27
3	3.3.5	URL 过滤设置
3	3.3.6	MAC 地址过滤
3	3.3.7	IP 过滤设置
3	3.3.8	IP 过滤设置
3.4	VPN 设	32
3	3.4.1	IPSec 设置
3	3.4.2	OPENVPN 设置
3	3.4.3	PPTP 设置
3	3.4.4	L2TP 设置
3	3.4.5	GRE 设置
3	3.4.6	Certificate 的导入43
3	3.4.7	VPN 日志
3.5	接口讨	殳 <u>置</u> 45
3	3.5.1	RS232 设置45
Ĵ	3.5.2	RS485 设置46
Ĵ	3.5.3	Profile Management (采集地址配置)48
Ĵ	3.5.4	FTP/SFTP Server 设定48
3.6	System	
Ĵ	3.6.1	Name and Password49
3	3.6.2	NTP Server <i>设置</i>
£	3.6.3	Firmware Upgrade (固件升级)51
£	3.6.4	Backup & Restore (配置备份和恢复)51
Ĵ	3.6.5	System Reboot
£	3.6.6	SD Card
£	3.6.7	Network Diagnosis
第四章	£ 应用	教程54
4.1	通过	FTP Server 收集 VR301 采集的数据
4.2	IPSEC	的应用场景
4.3	L2TP	配置场景

第五章 VR301 与第三方 VPN 路由器对接配置64
5.1 华为 VPN 路由器与 VR301 的配置64
5.1.1 华为MSR900 与VR301 的GRE(带隧道密匙)配置64
5.1.2 华为MSR900 与VR301 的GRE(不带隧道密匙)配置
5.1.3 华为MSR900 与VR301 的IPSec(PSK 方式)配置67
5.1.5 华为 AR151 与 VR301 的 Ipsec(PSK)配置70
5.1.6 华为AR201 与VR301 的IPsec(PSK)配置73
5.1.7 华为AR151 与VR301 的L2TP 配置77
5.2 思科 VPN 路由器与 VR301 的配置80
5.2.1 思科 RV130W 与 VR301 的 IPSec(PSK)配置80
5.2.2 思科 RV325 与 VR301 的 IPSec(PSK)配置83
5.3 飞塔 Fortinet
5.3.1 飞塔 FG100D 与 VR301 的 IPsec (带证书)的配置87
6 福达 VPN 模块应用案例92
6.1 供水供水公司远程监控92
6.1.1 背景
6.1.2 方案概述
6.1.3 现场图片
6.2 包装生产线的 VPN 联网方案95
6.2.1 背景
6.2.2 组网方案
6.2.3 方案优势

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



	模块	VR-100 系列		VR-300 系列		
功能		VR-101H1-V	VR-101L1-V	VR-301H9-V	VR-301L1-V	VR-301L5-V
联	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
M	有线网接入	支持	支持	支持	支持	支持
方	Wifi (Client)	土林	古姓	NA	NA	NA
式	win (client)	×14	×14	NA	NA	NA
硬	RS232	1 [©]	1.	1	1	1
件	RS485	1	1	1	1	1
接	以太网口	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN	1WAN+4LAN
VPN	IPSec Client	支持(不带证书)	支持(不带证书)	支持	支持	支持
功	IPsec Server	NA	NA	支持	支持	支持
能	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	SPI 防火墙	支持	支持	支持	支持	支持
火	DMZ	支持	支持	支持	支持	支持
墙	端口映射	支持	支持	支持	支持	支持
功	端口触发	支持	支持	支持	支持	支持
能	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	MODBUS TCP	NA	NA	网口	図口	网口
议	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

福达 VPN 路由器选型表

Ps: (1) 令作为硬件预留接口,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



1.3.4 安装尺寸

单位: mm





9

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】

						- • •
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	有控制面板项 🕨 网络和共享中心			- - ⁴ y	搜索控制面板	Q
控制面板主页	查看基本网络信息并设置连	接				0
更改适配器设置	📃 ——	- 📭 -	🎱	查看完整映射		
更改高级共享设置	CNXMDNIPC050 (此计算机)	网络 49	Internet			
	查看活动网络			— 连接或断开连接		
	网络 49 工作网络		访问类型: Internet 连接: 🔋 本地连接			
	更改网络设置					
	设置新的连接或网络 设置无线、宽带、拨号、能	師町或 VPN 连接;或说	2置路由器或访问点。			
	连接到网络 连接到或重新连接到无线、	有线、拨号或 VPN 网	网络连接。			
另请参阅	选择家庭组和共享选项 访问位于其他网络计算机上	_的文件和打印机,或夏	更改共享设置。			
Internet 选项	Final State at sta					
Windows 防火墙 家庭组	疑难解答 诊断并修复网络问题,或范	行得故障排除信息。				

点击【更改适配器设置】



右键"本地连接"



点击【属性】

↓ 本地连接 属性
网络 身份验证 共享
连接时使用:
💇 Intel (R) Ethernet Connection I217-V
✓ SIMATIC Industrial Ethernet (ISO) ✓ PROFINET IO RT-Protocol V2.0 ✓ A PROFINET IO RT-Protocol V2.0 ✓ A Transat thit/版本 6 (TCP/TPa6)
 ✓ <u>Internet 协议版本 4 (TCP/IP+4)</u> ✓ ▲ 链路层拓扑发现映射器 I/O 驱动程序 ✓ ▲ 链路层拓扑发现响应程序
4 III >
安装 (20) 卸载 (1) 属性 (2)
描述 TCP/IF。该协议是默认的广域网络协议,它提供在不同 的相互连接的网络上的通讯。
确定即消

选中"Internet 协议版本 4 (TCP/IP V4)",点击【属性】

Internet 协议版本 4 (TCP/IPv4) 属性		? 🗙
常规 备用配置		
如果网络支持此功能,则可以获取自动您需要从网络系统管理员处获得适当的	指派的 IP 设 IP 设置。	置。否则,
 ● 自动获得 IP 地址 (Q) ● 使用下面的 IP 地址 (S): 		
IP 地址(I):		
子网掩码 (U):		
默认网关 (2):		
◎ 自动获得 DWS 服务器地址(B)		
─── 使用下面的 DNS 服务器地址 @):		
首选 DMS 服务器 (2):		
备用 DNS 服务器(A):		
□ 退出时验证设置 (L)		高級(2)
-	确定	

修改为手动,修改后 IP 如下:

Internet 协议版本 4 (TCP/IPv4) 属性	? ×
常规	
如果网络支持此功能,则可以获取自您需要从网络系统管理员处获得适应	自动指派的 IP 设置。否则, 当的 IP 设置。
◎ 自动获得 IP 地址(0)	
IP 地址(L):	192 .168 . 1 . 20
子网摘码(U):	255 . 255 . 255 . 0
默认网关 ⑪:	
◎ 自动获得 DMS 服务器地址(B)	
● 使用下面的 DNS 服务器地址 @	D:
首选 DNS 服务器 (2):	
备用 DMS 服务器(A):	· · ·
□ 退出时验证设置 (L)	高级(2)
	确定取消

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)

@ http://192.168.1.1/login.html	
---------------------------------	--

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)

Jser Name	
assword	
	LOGIN

3. 登录后将会显示状态画面下的网络连接状态

VR-3001	STATUS	NETWORK	FIREWALL	VPN	INTERFACE	SYSTEM	
	_						
	Network Stat	tus network info	rmation				
Network		Network Status					
Device	I Connect	ion					Descent
Log							Reconnect
	Connection Typ	ve WAN	WAN N	1ode	DHCP		
	IP Address		Netwo	rk Mask			
	Gateway Addre	ess	Primar	y DNS			
	Secondary DN	s					
	II LAN						
	LAN IP Addres	s 192.10	58.1.5				
	LAN1-Status	Down	LAN2-	Status	Up		
	LAN3-Status	Down	LAN4-	Status	Down		
	I Traffic S	tatistics					
	Cellular Link1-	Sent 0 byte	s Cellula	r Link1-Received	0 bytes		
	Cellular Link2-	Sent 0 byte	s Cellula	r Link2-Received	0 bytes		
	WAN-Sent	12582	bytes WAN-F	Received	83196 bytes		



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。

✿ STATUS > Network Status

Connection				Reconnect
Connection Type	WAN	WAN Mode	DHCP	
IP Address	0.0.0.0	Network Mask	0.0.0.0	
Gateway Address	0.0.0.0	Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0			
≣ LAN				
LAN IP Address	192.168.1.1			
LAN1-Status	Down	LAN2-Status	Up	
LAN3-Status	Down	LAN4-Status	Down	
Traffic Statistics				
Cellular Link1-Sent	0 bytes	Cellular Link1-Received	0 bytes	
Cellular Link2-Sent	0 bytes	Cellular Link2-Received	0 bytes	
WAN-Sent	0 bytes	WAN-Received	0 bytes	

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。

Basic Device Type: DX3001 DX3001_DA90 Device Name: S/N: DXL3001116140010 I Version DX3001 Hardware Version 2016-03-14 04:28:44 PM Release Date: Firmware Version: DX3001-0.8.1.2-2016-05-19 Upgrade Date: 2016-05-19 02:33:39 I Resource Usage CPU Usage: 6% Total Memory: 121696KB Memory Used: 93144KB Memory Usage: 76% SD Card Status: SD Card Capacity: 0 SD Card Usage: 0

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

● 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	己使用的存储
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。

✿ STATUS > Device Logs

🖩 Log Type

Informative log
 OWarning log
 Debug log

🖩 Log Content

		Refresh	Clear	Download
Timestamp	Content			
May 19 05:44:04	syslog.info syslogd started: BusyBox v1.22.1			
May 19 05:44:12	user.info WATCHDOG[1488]: watchdog enabled!			
May 19 05:44:12	user.info SMSTrigger: [SMSTrigger:]SMSTrigger run in /dev/ttyUSB1 115200 mode.			
May 19 05:44:12	user.err SMSTrigger: [SMSTrigger:]Open FIFO failed.FD value:-1 errno:2 retry : 0!			
May 19 05:44:12	authpriv.warn dropbear[1490]: Failed loading /etc/dropbear/dropbear_dss_host_key			
May 19 05:44:12	authpriv.warn dropbear[1490]: Failed loading /etc/dropbear/dropbear_ecdsa_host_key			
May 19 05:44:12	authpriv.info dropbear[1536]: Running in background			
May 19 05:44:13	user.info collection: main.c(517)-main: argc=4			
May 19 05:44:13	user.info collection: main.c(518)-main: Path: /var/collection			
May 19 05:44:13	user.info collection: main.c(519)-main: File rotate: 20			
May 19 05:44:13	user.info collection: main.c(520)-main: Interval: 5			
May 19 05:44:13	user.info gre_app: [GRE_APP] gre_app start			
PREV 1 2 3 4 5 NEXT				

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.

Connection Priority

Primary Connection	WAN 🔻
Secondary Connection	Disable 🔹
Tertiary Connection	Disable 🔻
Auto Detect	Ping 🔻
Target Address 1	114.114.114.114
Target Address 2	8.8.8.8
Dial Failure To Restart	Disable 🔻

Save

Cancel

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

Cel	lul	ar	Lin	k1

Operator	Auto 🔻
User Name	
Password	
APN	3gnet
Authorization Mode	Auto 🔻
Dial-Up Number	*99#(UMTS/3G/3.5G)
Dial-Up Mode	Always online
Redial Interval	30 (second)
Redial Times	0 (0 means always redial)
Max Idle Time	0 (0 means always online)
Connection Check Interval	60 second (0 means not checked)
Connection Check Times	5
MTU	1492

Save

Cancel

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

福达新创通讯科技(厦门)有限公司

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)	Always online
● Manual connection: 如果断开后,需要手动连接	
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
ΜΤυ	
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

爺 NETWORK > WAN

I WAN Settings

WAN Mode	DHCP •
IP Allocation Method	Dynamic 🔻
IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway Address	0.0.0.0
Packet MTU	1500
(Don't change the settings unl	ess really need to)
Retrieve DNS Address By:	Dynamic 🔻
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Save	Cancel

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.	DHCP
● 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	
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	рнср
信息.	Diloi
● 手动指定: 手动指定 IP 地址、掩码、网关等相关信息	
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
МТО	-
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	DHCP
只能选择"手动指定"	
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。

爺 NETWORK > LAN

I LAN Settings

IP Address	192.168.1.1
Network Mask	255.255.255.0
DHCP Server	Enable •
Address Lease Time	One day 🔹
First IP Address	192.168.1. 100
Last IP Address	192.168.1. 200
STP	Enable v

Save

Cancel

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。

fIREWALL > Basic

Basic Firewall Settings			
Firewall	Enable 🔻		
WAN Ping	Not response	•	
LAN SSH	Enable 🔻		
WAN SSH	Disable 🔻		
		Save	Cancel

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。

≣ DMZ				
DMZ Server	Enable 🔻			
DMZ Host IP Address				
		Save	Cancel	
				1
	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

					Add A Portforward Rule
ID	Service Name	Protocol	Public Port	Server Port	Server IP Address

点击"Add A Portforward Rule"后将看到如下页面。

Add A Portforward Rule

Network Services	Customized	•	
Service Name			
Protocol	TCP/UDP •		
Public Port	Single port 🔹	(1~65534)
Server Port	Single port <	(1~65534)
Server IP Address	192.168.1.		
	Save	Back	

	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, 头,字符串最大长度为 32 个	名称由字母、数字,下划线组成,以字母或数字开 字节。	N/A
Protocol		1
选择端口映射协议类型,	可选值 "TCP/UDP","TCP","UDP"。	TCP/UDP
Public Port		1
设置外部主机(即路由器 择指定端口范围时,端口范围) 意,别使用常规已经定义的端)端口,可指定"单一端口"或"端口范围";选 为 1~65534,起始端口必须小于等于结束端口。(注 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 2. 当外部端口选择"端口 "端口范围"。 3. 选择"单一端口",则: 4. 选择"端口范围",则: 不同端口映射设置结果示例: 1:1 模式 Public Port Server Port N:1 模式 Public Port Server Port N:N Public Port Server Port	-端口"模式,映射端口只能选择"单一端口" 1范围"模式,映射端口可选择"单一端口"或者 外部所由端口范围都映射到单一端口上。 端口范围和外部端口范围一致,并一一对应映射。 Single Port ▼ 1001 (1~65534) Single Port ▼ 80 (1~65534) A Port Range ▼ 1001 - 1008 (1~65534) Single Port ▼ 80 (1~65534) A Port Range ▼ 1001 - 1008 (1~65534)	Single Port
Server IP Addres		1
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

福达新创通讯科技 (厦门)有限公司

服务名	协议	起始端口	结束端口
Customized	TCP, UDP, TCP/UDP	1~65534	1~65534
FTP	ТСР	20	21
нттр	ТСР	80	80
ICUII	ТСР	23566	23566
IP_PHONE	ТСР	6670	6670
NetMeeting	ТСР	1720	1720
News	ТСР	119	119
РРТР	TCP/UDP	1723	1723
Telnet	ТСР	23	23
Quakell/III	TCP/UDP	27960	27960
Real-Audio	ТСР	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。

Port	Trigger Disable 🔻	Port Trigger Timeou	ıt 20	Minute	Save	Add A Trig	gger Rule	
ID	Service Name	Service Type	Inbound Conne	ction	Serv	ice User	Status	

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

🗮 Add A Trigger Rule	
Service Name	
Service User	Any address 🔻
Service Type	•
Trigger Port	(1~65534)
Inbound Connection	
Protocol Role	¥
Begin Port	(1~65534)
End Port	(1~65534)
Status	T
	Save Back

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"。	ТСР
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。

URL Address Filter Disable 🔻 Save		Add	Add An URL Address	
ID	URL Address	LAN IP Address	Status	

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

🗏 Add URL

URL Address		
LAN IP Address	Any address	•
Status	Enabled •	
	Save	Back

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。

▲ FIREWALL > MAC Filter MAC Filter Disable ▼ Save Add A MAC Address ID MAC Address Device Name Status 点击 "Add A MAC Address" 按钮后,你将会看到如下的页面。 ▲ FIREWALL > MAC Filter

🗮 Add A MAC Address		
MAC Address		
Device Name		
Status	Enabled v	
	Save	Back

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。

IP Filter Disable V Save					Add An IP A	Address	
ID Source IP Source Port Range Of Destination Range Of Protocol S Address Range Range IP Address Destination Port				Status			

点击"Add An IP Address"按钮后看到如下的页面。

🗏 Add An IP Address

Source IP	Any address 🔹	
Source Port	Any address	
Destination IP	Any address	
Destination Port	Any address 🔻	
Protocol	TCP/UDP 🔻	
Status	Enabled •	
	Save	Back

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

添加规则

浴 防火墙设置 > 网络地址转换 (NAT)

ID	动作	源网络	转换类型	匹配地址	转换地址	操作
1	SNAT	Inside	IP to IP	192.168.3.11	192.168.5.1	<u>编辑</u> <u>删除</u>
2	DNAT	Outside	IP to IP	192.168.5.1	192.168.3.11	<u>编辑 删除</u>

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
	可选项: SNAT/DNAT
动作	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
海网 级	可选项: Inside/Outside
你們给	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。

 \hat{m} VPN > IPSec Setting

I Connection Management						
AT Traversal:		Enabled	Save			
Name	Enabled	Status	Local Interface	Local Subnet	Peer Subnet	Operation

点击"ADD"后,

 $\hat{\mathbf{m}}$ VPN > IPSec Setting

IPSec Setting			
Name:		Enable:	False •
IPSec Type:	Net-to-Net	IPSec Role:	Client •
Local WAN Interface:	WAN	Peer WAN Address:	
Local Subnet:	/	Peer Subnet:	/
Local ID:		Peer ID:	
Phase1			
IKE Encryption:	3DES 🔻	IKE Integrity:	MD5 •
IKE DH Group:	Group2(1024)	IKE Lifetime:	120 (120-86400sec.)
≣ Phase2			
ESP Encryption:	3DES 🔻	ESP Integrity:	MD5 •
PFS:	Enabled •	ESP Keylife:	120 (120-86400sec.)
DH Group:	Group2(1024) •]	
🗏 Advanced			
Negotiation Mode:	Main Mode 🔹	IP Compress:	Enabled •
DPD Detection:	Enabled •	Time Interval:	60 (Sec.)
Timeout:	60 (Sec.)	DPD Action:	Hold
■ Authentication			
Use A Pre-Shared Key:			
Use The X.509 Cert:			
		Add Cancel	

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 Туре	
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 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(10 24)
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。

爺 VPN > OpenVPN

🗏 Basic Settings

OpenVPN Mode	Client •		
OpenVPN Server]	
Port	1194	Protocol	UDP •
Tunnel Device	TUN	Encryption	Blowfish CBC •
Advanced Setting	Enable •]	
LZO Compression	Disable •	NAT	Disable •
Local IP Address] мти	1500
TCP MSS		TLS Cipher	Enable •
Import TLS Auth Key	选择	全件 未选择文件	mport
Authentication			
• User:		Password:	
Use The X.509 Cert:		¥	

e Cancel

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。	TUN
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。	
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	
ΜΤυ	
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。

爺 VPN PPTP

🗏 Basic Settings

PPTP Mode	Client •	
PPTP Server]
User Name]
Password		Unmask
Obtain IP	Auto 🔻	
IP Address	0.0.0.0	
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
DNS	0.0.0.0	
Authorization Mode	Auto 🔻	
MPPE	Disabled •	
NAT	Disabled •	
MTU	1420	(576-1420)
Connection Check Interval	60	Sec(0 means not checked)
Connection Check Times	5]
Connection Status	Connecting	

Savo	
Jave	

Cancel

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
	МРРЕ	
	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	
断约	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 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。

Basic Settings

L2TP Mode	Client •	
L2TP Server]
User Name]
Password		Unmask
Obtain IP	Auto 🔻	
IP Address	0.0.0.0	
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
DNS	0.0.0.0	
Authorization Mode	Auto 🔻	
MPPE	Disabled v	
NAT	Disabled v	
MTU	1460	(576-1460)
Connection Check Interval	60	Sec(0 means not checked)
Connection Check Times	5]
Encryption	Disable •	
Connection Status	Connecting	

	确定	取消
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
МРРЕ	
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
МТО	
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	

Add

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。 ✿ VPN > GRE

Tunnel Name Status Tunnel Inter	face Src IP/Mask	Tunnel Inter	face Dst IP/Mask	Peer Subnet	Operation
爺 VPN > GRE					
Tunnel Setting					
Tunnel Name					
Enable Tunnel	Yes 🔻				
Tunnel Interface Src IP/Mask			/		
Tunnel Interface Dst IP/Mask			/		
Tunnel Based Src IP					
Tunnel Based Dst IP					
Peer IP Address/Mask			/		
Tunnel Key			(option,0-42949	967296)	
Connection Check Interval	0		Sec.(0 means r	not checked)
Connection Check Times	3				
		Save	Cancel		

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	<u>~</u>

默认值
Yes
0
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	
â	VPN >	Certificate	Management				

Connection Management

Group Name	CA	Public Cert	Private Cert	Expired Date	Operation
			Add		

☆ VPN > Certificate Management



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。

VPN Setting VPN Log

爺 VPN > VPN Log

🖩 VPN Log

Download the logs of VPN function to local PC. Specify logs of

IPSec •

Donwload

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。

I RS232 Configurations

Working Mode	Master mode ▼
Baud Rate	9600 🔻
Data Bits	8 🔻
Stop Bits	1 🔻
Parity Bits	None T
Flow Control	None •
Modbus Mode	ModBus RTU V
Modbus Timeout	1000
Retry Times	1

Save	Cancel
Curt	Curroor

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
● Close: 关闭该功能	
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。

=	RS485	Configuration
	1000	configuration

Working Mode	Master mode 🔻	·]	
Baud Rate	9600 🔻		
Data Bits	8 🔻		
Stop Bits	1 🔻		
Parity Bits	None ▼		
Modbus Mode	ModBus RTU	•	
Modbus Timeout	1000	(50/	~2000ms)
Retry Times	1	(1~	10)
		Save	Cancel

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
● Close: 关闭该功能	
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。

â	INTERFACE	>	Profile	Setting
---	-----------	---	---------	---------

				选择文件 未诜	择文件	Import	Caned	
						import	Cance	
Profile ID	Profile Interface	Profile Enable		File Name		Operat	ion	
				Add				
INTE	RFACE > Profile S	etting						
File	Setting							
rofile ID	D: 0	1	•					
nterface	e: F	RS232 •		Profile Enable: False		¥		
ile Nam	e Prefix:			File Name:	File Name: rawData			
File Name Postfix: MM-dd-yyyy-l		/M-dd-yyyy-ł	nh-mm-ss ▼	Separation Sign:	_		•	
∎ Inte	erface Setting							
lave ID	. 1			Intervalu	300		(c)	
lave ID	•			Interval.	300		(3)	
∎ File	Content							
			Function					
10.	Item Name		Code	Start Addr	Count	Enable		
1			01 🔻			True •	+	

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。

☆ INTERFACE > FTP/SFTP Server Setting

ETP/SFTP Server		
Upload Mode	FTP V	
Target Server		(IP or domain name)
Port	21	
File Path	/	
Account	deltauser	
Password	••••••	Unmask

Save	Cancel
------	--------

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。

	assword	
Device Name Setting		
Device Name	DX3001_DA90 Save	Cancel
🗏 Change Administrator P	Password	
Old Password		
New Password		
The password must be a comb	vination of 5 to 12 characters,numbers and	underline marks
Confirm Password		
	Save Cancel	
	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察	"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。 ✿ SYSTEM > Time Settings

The current time of device 2016-05-19 09:38:56

NTP Server:	time-nw.nist.gov Microsoft,Redmond,Washington			
		Save	Cancel	

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。

🗏 System Upgrade

DO NOT turn off the power supply or reboot the device during the upgrade process. Please select the correct firmware package which is consistent with the device model,otherwise the device may be damaged ! (Before upgrade the firmware, please backup the settings and data. Please contact the local dealers or

manufacturers when failed to upgrade the firmware)

Cal		_	
50	IPCT	Firmware	
		1 11 11 11 11 10 10	

选择文件 未选择任何文件

Upgrade	Cancel

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。

Backup & Restore

Device configurations ca	an be backed up and sa	aved to loc	al PC	
				Backup
Configuration restoratio configurations in your .c	n will remove the curre cfg file	ent setting	s in the device and restore t	:he
Select .Cfg File		Browse		
				Restore

Configurations will be reset to the factory default settings, device will be reboot after the reset

Reset To Factory Default

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

爺 SYSTEM > System Reboot

🗏 System Reboot

The network will be temporarily shut down during system reboot, please wait!

Restart Device

3.6.6 SD Card

用户可以通过改页面对 SD 卡进行管理

♠ SYSTEM > SD Card			
🖩 SD Card Setting			
Storage Limit	90 %	Save	
🗏 Format SD Card			

Format the SD card, the data will be completely removed!

Format SD Card

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。

✿ SYSTEM > Network Diagnosis

🖩 Network Diagnosis

Diagnosing Method	Ping Test •		
Host Name/IP Address		Start	
			*
			-
4			► /i

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。

3CDaemon					
<u>File View H</u> elp					
TFTP Server	Start Time	Peer	Bytes	Status	
FTP Server					
Configure FIF Server					
GO					
FTP Server is stopped. Click here to start it.					
Logging to Ftpd.log. Click to stop.					
X					
Not debugging. Click to start.					
Clear list. 🔽					
Syslog Server					
TFTP Client					
For Help, press F1					

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

3CDaemon Configu	iration	X
General FTP Pr	Configuration ofiles	TFTP Configuration Syslog Configuration
anonymous deltauser deltausr To add a profii "Save Profile"	User Info Profile User This user can: User User User Upload	anonymous Set/Change user's password D:\demo1\ Save Profile te Highlighted Pros mation into the form then press
JCDaemon	ile: Highlight the prof	nle, make your changes, then press 确定 取消 应用(A)

配完成后点击应用,然后返回到主界面。点击 🔝 启动 FTP 服务。

3CDaemon					
<u>File View H</u> elp					
TFTP Server	Start Time	Peer	Bytes	Status	
	Jun 28, 2018 13:14:35	local	0	Stopped TFTP Server	
	Jun 28, 2018 13:13:37	local	0	Listening for TFTP requests on IP address: 169.254.197.27, Port 69	
Configure TFTP Server	Jun 28, 2018 13:13:37	local	0	Listening for TFTP requests on IP address: 192.168.1.100, Port 69	
	Jun 28, 2018 13:13:37	local	0	Listening for TFTP requests on IP address: 192.168.145.9, Port 69	
GO					
TFTP Server is stopped. Click here to start it.					
Logging to Tftpd.log. Click to stop.					
X					
Not debugging. Click to start.					
Clear list.					
· · ·					
FIF Server					
Syslog Server					
TFTP Client					
For Help, press F1					

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:

福达新创通讯科技(厦门)有限公司

300 3CDaemon	-			
<u>File View H</u> elp				
TFTP Server Start Time	Peer	Bytes	Status	
FTP Server Jun 28, 2018 15:0	6:00 local	0	Listening for FTP requests on IP address: 169.254.197.27 Port 21	
Jun 28, 2018 15:0	6:00 local	0	Listening for FTP requests on IP address: 192.168.1.100, Port 21	
Jun 28, 2018 15:0	6:00 local	0	Listening for FTP requests on IP address: 192.168.145.9, Port 21	
Configure FTP Server				
FTP Server is started.				
Click here to stop it.				
Logging to Ftpd.log. Click to stop.				
X				
Not debugging. Click to start.				
Clear list.				
Syslog Server				
TFTP Client				
For Help, press F1				

设置 DX301 内部 TFTP 配置。配置完成后点击【Save】

VR-301	STATUS	NETWORK	FIREWALL	VPN	INTERFACE	SYSTEM					
	ETD/SETD	Configur	ation of ETD/SETD Sonvor								
RS232			auon or FTP/SFTP Server								
RS485	INTERFACE > FIP/SFTP Server Setting										
Profile Management	≣ FTP/S	III FTP/SFTP Server									
ETD/SETD Sorrer	Upload Mode	9	FTP •								
FTP/SFTP Server	Target Serve	er	192.168.1.100	(IP or don	nain name)						
	Port		21								
	File Path		/								
	Account		admin								
	Password		•••••	Unmask							
			Si	ave Ca	ncel						
—————————————————————————————————————	-										
能直 Profile 的应用	IJ										
ST	ATUS NETW	ORK FIRE	WALL VPN	INTERFAC	SYSTEM						
Beaca	Profile Setting Co	onfiguration of Profile	2								
K5232	爺 INTERFACE > Pr	ofile Setting									
RS485											
Profile Management	≡ Profile List										
FTP/SFTP Server					选择文件未选择任何文件	Import Cancel					
	Profile ID Profi	le Interface	Profile Enable	File Nam	e	Operation					
				Add							

点击"ADD"按钮。设置 modbus TCP 的资料的采集资料如下。

Profile Setting Configuration of Profile

爺 INTERFACE > Profile Setting

≣ File Setting			
Profile ID:	01 🔻]	
Interface:	LAN.Modbus.TCP.Mas v	Profile Enable:	True 🔻
File Name Prefix:	modbusTCP	File Name:	TCPdata
File Name Postfix:	Unix Timestamp 🔹	Separation Sign:	_ *
Interface Sett	ing	,	
Target IP Address:	192.168.1.5	Port:	502
Interval:	300	(s)	
EFile 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:

3CDaemon					
<u>File V</u> iew <u>H</u> elp					
TFTP Server	Start Time	Peer	В	Status	
FTP Server	Jun 28, 2018 16:08:40	192.168.1.1	124	221 Service closing control connection	
	Jun 28, 2018 16:08:30	192.168.1.1	124	221 Service closing control connection	
<u></u>	Jun 28, 2018 16:08:20	192.168.1.1	124	221 Service closing control connection	
Configure FTP Server	Jun 28, 2018 16:08:10	192.168.1.1	124	221 Service closing control connection	
	Jun 28, 2018 16:08:00	192.168.1.1	124	221 Service closing control connection	
5TOP	Jun 28, 2018 16:07:50	192.168.1.1	124	221 Service closing control connection	
	Jun 28, 2018 16:07:40	192.168.1.1	124	221 Service closing control connection	
Click here to stop it.	Jun 28, 2018 16:07:30	192.168.1.1	124	221 Service closing control connection	
	Jun 28, 2018 16:07:20	192 168 1 1	124	221 Senice closing control connection	
	Jun 28, 2018 15:06:00	local	0	Listening for FTP requests on IP address: 169.254.197.27, Port 21	
	Jun 28, 2018 15:06:00	local	0	Listening for FTP requests on IP address: 192.168.1.100, Port 21	
Logging to Ftpd. Log. Click to stop.	Jun 28, 2018 15:06:00	local	0	Listening for FTP requests on IP address: 192.168.145.9, Port 21	
<u>.</u>					
Not debugging. Click to start.					
Clear list					
▼ Susles Server					
TFTP Client					
For Help, press F1					

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
	0040 05 00 45 00	1.0 0.000	4.100

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。

_ н	В	
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

) ① 🗞 https://192.168.5.	1/view/main/default.html?Vorsion=1.2&pageid=81862	課 C Q 百宮・	<cut+k>: ☆自 本 合 ち - ね - ●</cut+k>
高达问 🔙 火机百方站点 🍯	● 新手工路 🥌 東川叫北 🔝 敷濁玉		
~~~ Web官t	里平百		当前用户:admin 圆保存 參報助 ①关于 🎦注的
2955.	* 您的位置:广始网互联 > 以大使口		
) 配置向导	以太援日		
局域网接入	以太適口列表	修改以太接口	
广域网互联	推束项: 唐DS称 - Q.爱	当前接口模式:	电
以太田口	- 新語 │ × 形於│ 10 別所	自协商:	● 供能 ◎ 去供能
DSL接口	🔄 接口名称 接口编述 接口使率( 双工 自防商 物理状态	IPv4 V	
3G/LTERED	Ethernet0/0/4 HUAWELAR 100 金双工 日开启 🥥 可F		
SA接口	□ [4] 4 [篇] 页共1页] > 月	證人方式:	<ul> <li>DHCP 配置从ISP处目动获得即增加</li> <li>Static 配置从ISP处存得的固定即增加</li> </ul>
CE1/CT1接口	4		◎ PPPoE 配置从ISP处获得的用户名及密码
E1/T1提口	1	* P地址:	27 . 154 . 225 . 18
PON接口		* 子网掩码:	255 , 255 , 255 , 252
逻辑接口		默认网关:	
3年日 <b>留</b> 份		首流DNS服务器:	218 85 152 99
P业务		各用DNS照体器-	218 85 157 99
安全		启用NAT:	●是 0否
QoS		MTU (bytes):	1500 (46~1610,数认编=1500)
			147 D.16

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

🗲 🛈 💫   https://192.168.	.1/view/main/default.html?Version=1.2&pageid=81862	✓ 課 C Q 百度 <ctrl+k></ctrl+k>	☆自∔合	5-5-9 =
🙆 最常访问 🔒 火狐官方站点	🔰 新手上路 📙 常用网址 💹 爱海宝			
AR Web管	理平台		当前用户: admin	▼ 參帮助 10 关于 123 注销
公督概范	(您的位置: 安全 > ACL > 基本ACL配置			
📮 配置向导	基本ACL配置 高级ACL配置 二层ACL配置 生效时间			
膏 局域网接入	基本ACL配置列表			
名 广域网互联	🕂 新建  🖏 刷新			
119 119 119 119 119	ACL	类型		操作
	€ 2001	IPv4		添加规则 🗙
XE	Ethernet0/0/4	IPv4	11-00-01720	添加规则 ×
AUL	2021年5 2017年 5 会社	線P/的吸伏度(通配符) 192168-2.0/0.0.0255	生双时间段	<b>操作</b>
初天海	E 6 允许	192.168.3.0/0.0.255	- none -	×
安主(0)94 851	7 允许	11.0.0.0/0.0.255	- none -	×
PKI	B c_Ethernet_004	IPv4		滚加规则 🗙
AAA	Ethernet0/0/8	IPv4		添加规则 🗙
上网行为管理	4 4   第 1 页共1页  ▶ ▶		当前显示第1到4条记录/一	共4条记录 每页 10 🗸 条
🔄 QoS				
ST VPN				
👧 系统管理				
\Lambda 用户管理	-			cu

a) 4/XAICLED	直列表							
「新建」	13 刷新							
ACL			类型				操作	
3000		IF	Pv4				添加规则	×
3001		If	Pv4				添加规则	×
c_Etherr	net0/0/4_2	IF	Pv4				添加规则	×
c_Etherr	net0/0/4_1	H	Pv4				添加规则	×
规则编号	语 源IP/前缀长度(通配符)	目的IP/前缀长度(通配符)	* 动作	*协议类型	源端口号	目的端口号	操作	
5	192.168.5.0/0.0.255	192.168.2.0/0.0.0.255	允许	IP	- <u></u>	<u></u>	高级 🗙	
6	192.168.5.0/0.0.255	192.168.3.0/0.0.0.255	允许	IP			高级 🗙	
c_ethern	net0/04_1	IF	Pv4				添加规则	×
p_Etherr	net0/0/8_1	If	Pv4				添加规则	×
14 4 1	第1 页共1页 ▶ 別				当前显示第1到6	备记录/一共6条记录	每页 10	v e

### (3) 配置 IPSec 服务器端的配置

Wohe							
And Mebil	理十百	修改IPSec 策略				×	当前用户:admin 圆保存 參帮助 ①关于 🖡
设备概范	> 양的位置: VPN > IPS	* IPSec连接名称:	center_vpn_1		(1~12个字符)	Â	
配置向导	TOSAC SERVICE	* 接口名称:	Ethernet0/0/4				
Ref El 10 1	a over same and	- 组网模式:	◎ 分支站点	(i) 91	時結点		
NUMBER (	IPSec 策略管理	IKE参数配置				1 1	
广域网互联	105のは19名か	IKE版本:	😐 v1	© v2			10.0-
P业务	Center vpn 1	协商模式:	◎ 主模式	• 野香	観式		
安全		认证方式:	◎ 预共享密钥	O RSA	数字证书		当前显示第1到1条记录/一共1条记录 每页 10 ×
0.05		预共享密钥:	•••••		(1~127个字符)	m	
405		认证算法:	MD5	~			
VPN		加密算法:	3DES	~	(该算法的安全级别任)		
IPSec VPN		DH组编号:	Group2	~			
L2TP VPN		IDSoc影物形器					
SSL VPN		I OCCERTICA					
VPN实例		安全协议:	ESP	*			
系统管理		ESP认证算法:	MD5	~		-	
用户管理		ESP加密算法:	3DES	~	(该算法的安全级别低)		
		封装模式:	<ul> <li>酸道模式</li> </ul>	() 传媒	裡式		

	Wob@III	πA				
2	And Menete	TP 1	修改IPSec 策略			×
	2048 HOLE	Charles Martin Contract	ESP加密算法:	3DES	★ (该算法的安全级别低)	^
128	(CM INFO	181的位置: VPN > IPS	封装模式:	◎ 隧道模式	◎ 传输模式	
9	配置向导	IPSec 策略管理				
Ţ	局域网接入	IPSec 装路营用	ACL名称:	c_Ethernet0/0/	4_2 ~	
-		+ ### X #64 5	高级≫			
8	/ 观网互联	◎ IPSec连接名称	本講身份类型:	◎ ℙ地址	<ul> <li>名称</li> </ul>	
	IP业务	Center vpn 1	对端名称:	DX3001	(1~127个字符)	
0	安全		NAT穿越:	☑ 启用		
-	0.5		DPD(失效对等体检测):	启用		
	Q05		作为Efficient VPN服务器:	启用		
胡	VPN		PFS:	- none -	~	
	IPSec VPN		IKE SA存活时间(秒):	86400	(60~604800,默认值=86400)	
	L2TP VPN		IPSec SA老化方式:	基于时间(秒) 36	00 (100~604800,默认值=3600)	
	SSL VPN			基于流量(KB) 18	443200 (0,2560~4194303,默认值=1843200)	
	VPN实例		路由注入:	12 白田		
-	系统管理		路由注入举型:	动态	*	
THE .			路由代朱纲·	60	(1~255.野认信=60)	
â	用户管理			00 		
			报义信息预提取;	日月用		-
				确定	取消	
				S		_

### 福达新创通讯科技(厦门)有限公司 福达 VPN 产品使用手册

分 设备概范	您的位置: VPN > IPSec V	/PN > IPSec 全	局设置		
🛄 配置向导	IPSec 策略管理 TPS	ec 全局设置			
膏 局域网接入	设备本地名称:	Huawei		(1~127个字符)	
名 广域网互联	IPSec SA 老化管理:	基于时间(秒)	3600	(100~604800,默认值=3600)	
🛄 IP业务		基于流量(KB)	1843200	(0,2560~4194303,默认值=1843200)	
💛 安全	IKE心跳发送间隔(秒):			(20~28800)	
🖻 QoS	IKE心跳超时时间(秒):			(60~28800)	
	NAT保存间隔(秒):	20		(5~300,默认值=20)	
33 VPN	· 抗重放:	☑ 启用			
IPSec VPN	IPSec隧道的DF位设置:	сору	,		
L2TP VPN	隧道报文加密前分片:	启用			
VPN		应用	重置	1	
	_				
▲ 用户管理					

- 2. VR301 的配置
- (1) 设置 WAN 口的连接为 SIM1

	STATUS	NETWORK	FIREWALL	VPN	INTERFACE	SYSTEM	EXT
Connection	Connect	ion Priority Setti	ng the internet connecti	on priority			
Cellular Link1	II NETW	VORK > Connection	Priority				p
Cellular Link2	III Conr	nection Priority					"Connection Priority Setting"
WAN	Primary (	Connection	Cellular Link1 V				u can set different priorities fo WAN/Cellular Link1/Cellular Li
LAN	Tertiary ( Auto Det	Connection	Disable •				so you can set the track ways t detect the network is online
	Target A	ddress 1	114.114.114.114				
	(must b	e public address, n ddress 2	8.8.8.8				
	(must b	e public address, n	ot vpn address)				
	Dial Failu	re To Restart	Disable 🔻				
	Detect In	nterval	60 (30~300s)				

(2) 配置 VR301 内部的 VPN 策略

	VPN Setting	Fetting			
PSec	WPN Security Security	ing .			VBN Setting Help
DenVPN	M THE PROCESSION	.9			vera setting rieip
	IPSec Setting				"IPSec Setting" You can add/d
PTP	in Trace setting				elete/modify the tunnel settin
TP	Name:	jipsec_huawei201	Enable:	Yes 🔹	he Local/Peer ID use IP/FQDN
	IPSec Type:	Net-to-Net *	IPSec Role:	Client •	like: 10.0.0.1,or @domain.com
RE	Local WAN Interface:	WAN *	Peer WAN Address:	27 154 225 18	When using Certificate, the Lo al/Peer ID use IP/FODN/DN or
	Local Subnet:	192.168.2.0 / 24	Peer Subnet:	192.168.5.0 / 24	Null, like: 10.0.0.1/@domain.co
cruncate	Local ID:	@DX3001	Peer ID:	(2Huawei	m/C=AU,ST=Some-State,O=In
PN Log	10000000	3	10000000	Sec. 1	rt upcase and lowcase in tunn
	II Phase1				I name, but not support the sa
	IVE Econoticos	ades v	IVE Integrity:	MD5 •	me characters Two kinds of VPN could not b
	ike endypoon.	0	the morginey.	400	started at the same time
	IKE DH Group:	Group2(1024)	IKE Lifetime:	(120-86400sec.)	Name: Input the name of IPSe
	1.000				ated with other connection's r
	III Phase2				ame. Name can be up to 20 ch
	ESP Encryption:	3DES .	ESP Integrity:	MD5 •	aracter long.
	PFS:	Disabled •	ESP Kevlife:	120 (120-86400sec.)	onnection.
	129/732		Name (South Cold)		IPSec Type: Setup the working
	<b>≡</b> Advanced				poort Net-to-Net only.
		Accession Marchan	1222	Disabled	IPSec Role: Setup the role of t
	Negotiation Mode:	Aggressive mode •	IP Compress:	Lisabled +	he router in IPSec.
	DPD Detection:	Enabled *	Time Interval:	60 (Sec.)	d WAN interface, system will a
	Timeout:	60 (Sec.)	DPD Action:	Restart 🔻	uto assign it base on connecti
					n status. Peer WAN Address: IP/domai
					. eel trait Address. IP/dolla

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



VR301 端的 GRE 配置如下

	STATUS NETWORK	FIREWALL	VPN INTERFAC
	VPN Setting Configuration	of I/DN	
IPSec	A VPN > GRE	DI VPN	
OpenVPN	III Tunnel Setting		
РРТР	Tunnel Name	Tunnel1	
L2TP	Enable Tunnel	True 💌	
ODE	Tunnel Interface Src IP/Mask	1.1.1.2	/ 24
UKE	Tunnel Interface Dst IP/Mask	1.1.1.3	/ 24
Certificate	Tunnel Based Src IP	192.168.1.102	
/PN Log	Tunnel Based Dst IP	192.168.1.103	
	Peer IP Address/Mask	192.168.3.0	/ 24
	Tunnel Key	123456	(option,0-4294967296)
	Connection Check Interval	10	Sec.(0 means not checked)
	Connection Check Times	5	

华为 MSR900 的 GRE 配置如下:

НЗС	Web Management	Platform	
N > GRE			
AH3C - 设备概览 	修改版道		
	Tunnel接口编号:	Tunnel1	
- 🖬 3G	IP地址/掩码:	1.1.1.3	/ 255.255.255.0 *
- DINAT配置	隧道源端地址/接口:	192.168.1.103	*
- 🔂 安全配置	隧道目的端地址;	192.168.1.102	*
高级配置	GRE密钥:	123456	(0-4294967295)
- VPN	GRE报文检验和功能:	禁用 ▼	
- IPsec VPN	■ 发送Keepalive报文:	启用 ▼	
GRE	发送Keepalive报文间隔:	10	秒(1-32767,缺省值=10)
SSL VPN	发送Keepalive报文次数:	5	(1-255,缺省值=3)
→ 証书管理 → PKI实体	星号(*)为必须填写项	确定 取満	

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)

- NATELE							
━ 安全配置		A172 HIRA	1				
一访问控制	322/31	College Uppeds					
-URL过滤	ENIPHAL	192 168 2 0	*				
- MAC地址过滤	 掩码	255.255.255.0	•		□ 优先级		(1-255,缺省=60)
- 🗈 攻击防范	 下 <b>—</b> 跳				☞ 接口	Tunnel1 Tunnel1	
一应用控制		5215					
高级配置	 997 ( ) /30%					确定	
一页面推送	 						
- 路由设置	 配置的静态路由信	鎴					
- 基于用户的负载分担	Designition						1
	EBUIPTURE	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	协议	优先级	下一跳	接口	
- 流晕统计排名	0.0.0.0	·	· 协议 Static	 60	下一跳 172.17.92.114	接口 Ethernet0/0	-
- 流量统计排名	0.0.0.0 0.0.0.0	· 推码 0.0.0.0 0.0.0.0 0.55 055 0	初议 Static Static	60 60 60	下一跳 172.17.92.114	接口 Ethernet0/0 Tunnel1	
ー流量统计排名 - ☎ DNS设置	0.0.0.0 0.0.0.0 192.168.3.0 192.168.6.0	: 掩码 0.0.0.0 0.0.0.0 255.255.255.0 255.255.255.0	初议 Static Static Static Static	优先级 60 60 60 60 60	下一跳 172.17.92.114	接口 Ethernet0/0 Tunnel1 Tunnel1 Tunnel1	L
<ul> <li>–流量统计排名</li> <li>–</li> <li>–</li> <li>→ DNS设置</li> <li>–</li> <li>→ DHCP设置</li> </ul>	0.0.0.0 0.0.0.0 192.168.3.0 192.168.6.0	· 推码 0.0.0.0 0.0.0.0 255.255.255.0 255.255.255.0	竹议 Static Static Static Static Static	60 60 60 60 60 60	下一跳 172.17.92.114	接口 Ethernet0/0 Tunnei1 Tunnei1 Tunnei1	
<ul> <li>- 流星统计排名</li> <li>- ⑤ DNS设置</li> <li>- DHCP设置</li> <li>- ⑥ QoS设置</li> </ul>	EBJ#7831 0.0.0.0 192.168.3.0 192.168.6.0	: 挿码 0.0.0.0 0.0.0.0 255.255.255.0 255.255.255.0	Static Static Static Static Static	优先级 60 60 60 60	下一部	接口 Ethernet0/0 Tunnel1 Tunnel1 Tunnel1 Tunnel1	L
<ul> <li>一流量统计排名</li> <li>- 副 DNS设置</li> <li>- DHCP设置</li> <li>- 副 QoS设置</li> <li>- 网桥</li> </ul>	BH30F7832 0.0.0.0 192.168.3.0 192.168.6.0	: 揮码 0.0.0.0 0.0.0.0 255.255.255.0 255.255.255.0	thiy Static Static Static Static	优先级 60 60 60 60	下一部 172.17.92.114	接口 Ethernet0/0 Tunnel1 Tunnel1 Tunnel1	L

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



VR301 端的 GRE 配置如下

#### 福达新创通讯科技(厦门)有限公司

福达 VPN	产品使用手册
--------	--------

PSec	on woocang configuration		
-000	☆ VPN > GRE		
penVPN	🔳 Tunnel Setting		
TP	Tunnel Name	Tunnel1	
P	Enable Tunnel	True 💙	
	Tunnel Interface Src IP/Mask	1.1.1.2	/ 24
	Tunnel Interface Dst IP/Mask	1.1.1.3	/ 24
icate	Tunnel Based Src IP	192.168.1.102	
.og	Tunnel Based Dst IP	192.168.1.103	
	Peer IP Address/Mask	192.168.3.0	/ 24
	Tunnel Key		(option,0-4294967296)
	Connection Check Interval	0	Sec.(O means not checked
	Connection Check Times	5	

MSR900 的 GRE 的配置如下:

VPN > GRE		
<b>В</b> нзс		
一设备概览	修改隧道	
一國快速向导	Tunnel接口编号:	Tunnel1
	IP地址掩码:	1.1.1.3 / 255.255.255.0 *
- C NAT配置	隧道源端地址/接口:	192.168.1.103
- 🔂 安全配置	隧道目的端地址:	192.168.1.102 *
高级配置	GRE密钥:	(0-4294967295)
	GRE报文检验和功能:	禁用 ▼
- IPsec VPN	发送Keepalive报文:	禁用 ▼
GRE	发送Keepalive报文间隔:	10 秒(1-32767,缺省值=10)
SSL VPN	发送Keepalive报文次数:	3 (1-255,缺省值=3)
一〇〇 证书管理	星号(*)为必须填写项	
— PKI实体		确定取消

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)

INATELE A								
●安全配置		470 BHEA						
一访问控制	512775	3022 JBR/F						-
URL <u>过</u> 滤	ERIPHAL 19	2 168 2 0	*					
-MAC地址过滤	推码 26	5.255.255.0	•		🔲 优先级		(1-255,缺省=60)	
■ 攻击防范	下一郎				☞ 接口	Tunnel1 •		
- 应用控制		5						
● 高级配置	生亏()为必须有一	×				确定		
一页面推送							1	
- 路由设置	配置的静态路由信息							
- 基于用户的负载分担	目的IP地址	掩码	协议	优先级	第一千	接口		
- 流量统计排名	0.0.0.0	0.0.0.0	Static	60	172.17.92.114	Ethernet0/0		
- 🔁 DNS设置	192.168.3.0	255.255.255.0	Static	60		Tunnel1		
- DHCP设置	192.168.6.0	255.255.255.0	Static	60		Tunnel1		
- De QoS设置								
573445								

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



#### VR301 的设置通过 SIM1 来上网

	STATUS	NETWORK	FIREWALL	VPN
	Connect	ion Priority Coi	tion the internet competion of	ri e vitu
Connection		/ORK > Connection	n Priority	noncy
Cellular Link1			,	
Cellular Link2	III Conn	ection Priority		
WAN	Primary C Secondar	connection	Cellular Link1 V WAN	
LAN	Tertiary C	Connection	Cellular Link1 Cellular Link2	
	Auto Dete	ect	Disable 🔽	
		Save	Cancel	

配置 SIM1 的 APN 参数

### 福达新创通讯科技(厦门)有限公司

Connection	Cellular	LINKI Keuleve ul		
Sonnoccion	🛧 NET	WORK > Cellular Link	1	
Cellular Link1				
Cellular Link2	III Cel	lular Link1		
WAN	Operato	or	Auto 🔽	
	User Na	ame		
LAN	Passwo	ord		
	APN		3gnet	
	Authoria	zation Mode	Auto 🛩	
	Dial-up	Number	*99#(UMTS/3G/3.50	G) 🔽
	Dial-up	Mode	Always online	*
	Redial I	nterval	30 (second)	
	Redial T	īmes	0 (0 means al	ways redial)
	Max Idl	e Time	0 (0 means alv	ways online)
	Connec	tion Check Interval	60 second (0 m	eans not checked)
	Connec	tion Check Times	5	
	MTU		1492	
置 VR301 的 I evice × ve ① 192.168.7.1/ind	PSec 参数 	638	_	
置 VR301 的   evice × ve ⑦ ① 192.168.7.1/ind	PSec 参数 HBC MSR 50 28曲巻-1 × ex.html?0.1065700584563 III IPSec Setting Name:	638. TT	Enable	Yes
置 VR301 的   evice × * ① 192.168.7.1/ind	PSec 参数 × H3C MSR 50 28曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type:	638 ttt Net-to-Net	Enable:	Yes •
置 VR301 的   avice × vr ① 192.168.7.1/ind	PSec 参数 Hac MSR 50 28曲巻-1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface:	638 ttt Net-to-Net WAN	Enable: IPSec Role: Peer WAN Address:	Yes • Client • 27.154.234.82
置 VR301 的 I	PSec 参数 H3C MSR 50 28曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet:	638 ttt Net-to-Net WAN 192.168.7.0 / 24	Enable: IPSec Role: Peer WAN Address: Peer Subnet:	Yes ▼ Client ▼ 27.154.234.82 192.168.1.0 / 24
置 VR301 的 I evice × v ② ③ 192.168.7.1/ind	PSec 参数 Hac MSR 50 缩曲器 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local ID;	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001	Enable: IPSec Role: Peer WAN Address: Peer Subnet: Peer ID:	Yes         ▼           Client         ▼           27.154.234.82         192.168.1.0           192.168.1.0         /           24         @H3C
置 VR301 的 I evice × ① 192.168.7.1/ind	PSec 参数 < H3C MSR 50 28曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local JD: III Phase1	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001	Enable: IPSec Role: Peer WAN Address: Peer Subnet: Peer ID:	Yes ▼ Client ▼ 27.154.234.82 192.168.1.0 / 24 @H3C
置 VR301 的 I evice × v ① 192:168.7:1/ind	PSec 参数 < H3C MSR 50 隨曲器 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Local JD; III Phase1 IKE Encryption:	638 ttt Net-to-Net WAN 192,168,7.0 / 24 @DX3001 3DES	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> </ul>	Yes ▼ Client ▼ 27.154.234.82 192.168.1.0 / 24 @H3C MD5 ▼
置 VR301 的 I	PSec 参数 < H3C MSR 50 額曲器 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local JD; III Phase1 IKE Encryption: IKE DH Group:	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001 3DES Group2(1024)	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> </ul>	Yes  Client Z7.154.234.82 192.168.1.0 / 24 @H3C MD5 I20 (120-86400sec.)
置 VR301 的 I	PSec 参数 < H3C MSR 50 隨曲器 - 1 × 《 ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Local JD: III Phase1 IKE Encryption: IKE DH Group:	638 ttt Net-to-Net WAN 192,168,7.0 / 24 @DX3001 3DES Group2(1024)	Enable: IPSec Role: Peer WAN Address: Peer Subnet: Peer ID: IKE Integrity: IKE Lifetime:	Yes          Client          27.154.234.82          192.168.1.0       /         @H3C          MD5          120       (120-86400sec.)
置 VR301 的 I	PSec 参数 < H3C MSR 50 28曲巻 - 1 × ex.html?0.1065700584563 III 1PSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Local Subnet: Local ID: III Phase1 IKE Encryption: IKE DH Group: III Phase2	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001 3DES Group2(1024)	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> </ul>	Yes  Client 7.154.234.82 192.168.1.0 / 24 @H3C MD5 120 (120-86400sec.)
置 VR301 的 I	PSec 参数 H3C MSR 50 隨曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Local JD: III Phase1 IKE Encryption: IKE DH Group: III Phase2 ESP Encryption: BCC	638 ttt Net-to-Net WAN 192,168,7.0 / 24 @DX3001 3DES Group2(1024) 3DES Epabled	Enable: IPSec Role: Peer WAN Address: Peer Subnet: Peer ID: IKE Integrity: IKE Lifetime: ESP Integrity: ESP Kodifie:	Yes       •         Client       •         27.154.234.82       192.168.1.0         192.168.1.0       /         @H3C       •         MD5       •         120       (120-86400sec.)         MD5       •         120       (120-86400sec.)
置 VR301 的 I	PSec 参数 * H3C MSR 50 38曲器 - 1 × * ex.html70.1065700584563 E 1PSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet:	638	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> </ul>	Yes          Client          27.154.234.82          192.168.1.0       /         24          @H3C          MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)
置 VR301 的 I	PSec 参数 H3C MSR 50 隨曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Local Subnet: Local ID: IIII Phase1 IKE Encryption: IKE DH Group: III Phase2 ESP Encryption: PFS: DH Group: III + + + + + + + + + + + + + + + + + +	638	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> <li></li> </ul>	Yes       •         Client       •         27.154.234.82       192.168.1.0         192.168.1.0       /         @H3C       •         MD5       •         120       (120-86400sec.)         MD5       •         120       (120-86400sec.)
置 VR301 的 I	PSec 参数 * H3C MSR 50 猶曲器 - 1 × * ex.html70.1065700584563 Ex.html70.1065700584563 H IPSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local S	638	Enable: IPSec Role: Peer WAN Address: Peer Subnet: Peer ID: IKE Integrity: IKE Lifetime: ESP Integrity: ESP Keylife:	Yes          Client          27.154.234.82          192.168.1.0       /         QH3C          MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)
置 VR301 的 I	PSec 参数 H3C MSR 50 28曲巻 - 1 ×  ex.html?0.1065700584563 III 1PSec Setting Name: IPSec Type: Local WAN Interface: Local Subnet: Local Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subne	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001 3DES Group2(1024) 3DES Enabled Group2(1024) Aggressive Mode Enabled	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> <li>IP Compress:</li> <li>The Lifetime in the second secon</li></ul>	Yes          Client          27.154.234.82          192.168.1.0       /         ØH3C       /         MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)         Disabled
置 VR301 的 I	PSec 参数 HaC MSR 50 隨曲巻 - 1 × ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local WAN Interface: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local WAN Interface: Local WAN Interface: Local Subnet: Local Subnet: DPI Group: III Advanced Negotiation Mode: DPI Detection: Time: T: Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet: Subnet:	638  ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001  3DES Group2(1024)  3DES Enabled Group2(1024)  Aggressive Mode Enabled 60 / rec. 1	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> <li>IP Compress:</li> <li>Time Interval:</li> <li>DPD Action:</li> </ul>	Yes          Client          27.154.234.82          192.168.1.0       /         ØH3C          MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)         Disabled          ©       (50         (120-86400sec.)
置 VR301 的 I	H3C MSR 50 38曲器 - 1 × 1         ex.html70.1065700584563         III IPSec Setting         Name:         IPSec Type:         Local WAN Interface:         Local Subnet:         Local Subnet:         Local Subnet:         Local File         III Phase1         IKE Encryption:         IFS:         DH Group:         III Advanced         Negotiation Mode:         DPD Detection:         Timeout:	638 ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001 3DES Group2(1024) 3DES Enabled Group2(1024) Aggressive Mode Enabled 60 (Sec.)	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> <li>IP Compress:</li> <li>Time Interval: DPD Action:</li> </ul>	Yes          Client          27.154.234.82          192.168.1.0       /         ØH3C       //         MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)         Disabled          60       (Sec.)         Hold
置 VR301 的 I	PSec 参数 HaC MSR 50 隨曲番 - 1 × 1 ex.html?0.1065700584563 III IPSec Setting Name: IPSec Type: Local WAN Interface: Local WAN Interface: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local WAN Interface: Local WAN Interface: Local WAN Interface: Local WAN Interface: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local Subnet: Local WAN Interface: Local WAN Interface: Local WAN Interface: Local Subnet: Local Subnet: Local WAN Interface: Local Subnet: Local Subnet: DPI Detection: Timeout: III Authentication	638  ttt Net-to-Net WAN 192.168.7.0 / 24 @DX3001  3DES Group2(1024)  3DES Enabled Group2(1024)  Aggressive Mode Enabled 60 (Sec.)	<ul> <li>Enable:</li> <li>IPSec Role:</li> <li>Peer WAN Address:</li> <li>Peer Subnet:</li> <li>Peer ID:</li> <li>IKE Integrity:</li> <li>IKE Lifetime:</li> <li>ESP Integrity:</li> <li>ESP Keylife:</li> <li>IP Compress:</li> <li>Time Interval: DPD Action:</li> </ul>	Yes          Client          27.154.234.82          192.168.1.0       /         ØH3C          MD5          120       (120-86400sec.)         MD5          120       (120-86400sec.)         Disabled          60       (Sec.)         Hold

#### 配置 MSR900 的 WAN 口参数

H3C					
设备概览	设置WAN口参数				
会快速向导	配置 WAN 日参数 以	(连接到 Internet			
接口配置	WAN 🗆	Ethernet0/0	r		
-WAN接口设置	接口状态	已连接	关闭		
-LAN设置	连接模式	手动指定IP地址	•		
■无线	TCP-MSS	1460	* (128 - 204	48,缺省=1460)	6.
3G	MTU	1500	* (46 - 1500	0, 缺省=1500)	
NAT配置	IP 地址	27.154.234.82	*		
安全配置	子网掩码	30 (255.255.255.252)	•		
- 访问控制	网关地址	27.154.234.81			
- URL过滤	DNS1	218.85.152.99			
- MAC地址过滤	DNS2	218.85.157.99			
🗈 攻击防范	MAC地址	● 使用本设备原来的MAC地	止(3822-d696	6-70c0)	
- 应用控制		◎ 使用下面手工输入的MAC	也址(如:000F	F-E254-F5E0)	
高级配置				確定	取消
页面推送				WDAE	-WIN

MSR900的隧道配置截图1

H3C Series Router MSF ×				and the second second	10.00		•	×
← → C ① 不安全   192.168.1	.1/wcn/frame/.x						9☆	0
нзс	Web Manager	nent Platform						
VPN > IPsec VPN						保存	帮助	退出
<ul> <li>- 贝血種法</li> <li>- 路由设置</li> <li>- 基于用户的负载分担</li> <li>- 流量统计排名</li> <li>- ● DNS设置</li> <li>- DHC002 面</li> </ul>	<mark>様女Psec法接</mark> IPsec法接名称 test 一 内关信息 接口	Ethernet0/0 •					-	-
- ¹ ² ² ³	一 阿关地址 对弹阿关地址/主机名 本课网关地址	27.154.234.82	字符(1 - 255)					
- 访问控制 ● ARP管理 ▲● ARP防攻击 ● VPN	- 以证 							
- IPsec VPN - IL2TP - GRE	新型約 碘以新密钥 ② 证书 网关ID	CN=routera *	李符(1 - 128)					
- THE	对碘ID类型	◎ IP地址 ● FQDN	对端网关ID	DX3001	* 李符(1 - 32)			
◎ 辅助工具	本族ID类型	◎ IP地址 ● FQDN	本端网关ID	H3C	* 字符(1-32)			

MSR900 的隧道配置截图 2

L'environne de la companya de	1.47.578				
- 网桥 - 60 群组管理	对读ID类型	<ul> <li>IP地址</li> <li>● FQDN</li> </ul>	对講网关ID	DX3001	* 李符(1 - 32)
- 访问控制 - 御 ARP管理	本端ID类型	◎ IP地址 ● FQDN ◎ User FQDN	本端网关ID	НЗС	* 李符(1 - 32)
VPN	一篇远器				
- IPsec VPN	筛运方式	流量特征▼			
- DI L2TP	源地址/通配符	192.168.1.0	0.0.255	•	
- GRE	目的地址/通配符	192.168.7.0	0.0.0.255	•	
■ 证书管理	反向路由注入	肝層 🖲 关闭			
■系统管理	▶高级 〒二 (*) 五次須接官項				
■ 辅助工具	#5( / /32/2045%		确定取	消	
MUNIO	-		L		

MSR900 的隧道配置截图 3

级 第一阶段		
交换模式	◎ 主模式 🖲 野蛮模式	
认证算法	MD5 🔻	
加密算法	3DES 🔻	
DH	Diffie-Hellman Group	2 🔻
SA的生存周期	86400	秒(60 - 604800,缺省值 = 86400)
ESP认证算法	MD5 T	
stativ	FSP V	
ESP加密算法	3DES V	
封装模式	<ul> <li>隧道模式</li> <li>传輸模式</li> </ul>	
PFS	Diffie-Hellman Group2	T
SA的生存周期		
基于时间的生存周期	3600	秒(180-604800,缺省值=3600)
	Top Menance Y	The set of

# 5.1.5 华为 AR151 与 VR301 的 Ipsec(PSK)配置



#### VR301 的设置通过 SIM1 来上网

	STATUS	NETWORK	FIREWALL VPN
	Connecti	on Priority Se	tting the internet connection priority
Connection		ORK > Connectio	n Priority
Cellular Link1			
Cellular Link2	I Conn	ection Priority	Internet in the second s
WAN	Primary C Secondar	onnection	Cellular Link1 🗸
LAN	Tertiary C	onnection	Cellular Linki Cellular Link2
	Auto Dete	ect	Disable 💌
		Save	Cancel

#### 配置 SIM1 的 APN 参数

O a mar a stila a	Cellular Link1 Retrieve th	e DNS server address from cellular network
Connection	🏦 NETWORK > Cellular Link	1
Cellular Link1		
Cellular Link2	I Cellular Link1	
MAN	Operator	Auto 💌
	User Name	
.AN	Password	
	APN	3gnet
	Authorization Mode	Auto 🔽
	Dial-up Number	*99#(UMTS/3G/3.5G)
	Dial-up Mode	Always online 💙
	Redial Interval	30 (second)
	Redial Times	0 (0 means always redial)
	Max Idle Time	0 (0 means always online)
	Connection Check Interval	60 second (0 means not checked)
	Connection Check Times	5
	MTU	1492
		Save Caprel
	I	

#### 设置 VR301 的 IPSec 参数

DIADevice ×			Contract Column and a	A DESCRIPTION OF THE OWNER.
← → C 🛈 192.168.1.1	1/index.html			
IPSec OpenVPN	VPN Setting IPSec S	setting Ig		
ротр	IPSec Setting			
L2TP	Name:	Huawei	Enable:	Yes v
	IPSec Type:	Net-to-Net •	IPSec Role:	Client
GRE	Local WAN Interface:	WAN •	Peer WAN Address:	27.154.234.82
Certificate	Local Subnet:	192.168.1.0 / 24	Peer Subnet:	192.168.2.0 / 24
	Local ID:	@DX3001	Peer ID:	@Huawei
VPN Log	III Dhacal			
	II Phasel			
	IKE Encryption:	3DES •	IKE Integrity:	MD5 V
	IKE DH Group:	Group2(1024)	IKE Lifetime:	120 (120-86400sec.)
	⊞ Phase2			
	ESP Encryption:	3DES 🔻	ESP Integrity:	MD5 •
	PFS:	Disabled •	ESP Keylife:	120 (120-86400sec.)
	i Advanced			
	Negotiation Mode:	Main Mode 🔹	IP Compress:	Disabled •
	DPD Detection:	Enabled •	Time Interval:	60 (Sec.)
	Timeout:	60 (Sec.)	DPD Action:	Hold •
	<ul> <li>Authentication</li> <li>Use A Pre-Shared Key:</li> </ul>	. 123456		

华为的 WAN 口设置

AR Web Platform ×			CONTRACTOR OF THE PARTY OF THE PARTY OF		
	ps://192.168.2.1/view/main/	default.html?Version=1.2	&pageid=272136		
AR Web Plat	tform		and the second second		Current User: admin 🛛 🗒 Save 🥏 Help
Pevice Information	Your Position : WAN Access	> Ethernet Interface			
Configuration Wizard	Ethernet Interface				
· LAN Access	Ethernet Interface List	Madifie The survey Takasfara		୍କ	
K WAN Access	Item: Interface Name	* Interface name:	Ethernet0/0/4	A	
Ethemet Interface DSL Interface SA Interface SA Interface Eti/T1 Interface Eti/T1 Interface Eti/T1 Interface Logical Interface Interface Backup Interface Backup Security Security Security Security Securits Secu	therefore the second sec	Description: Working Mode: Current Mode: Auto-negotiation: IP IP4 Connection mode: IP address: Subnet mask: Default gateway: Primary DNS server: Secondary DNS server:	HUAWEI, AR Series, Ether (1-242 characters) Electrical Electrical • Enable • Dicable • DHCP: Obtain IP addresses from the ISP • State: Obtain A fixed IP address from the ISP • PPPoE: Obtain the user name and password from the ISP 27 : 154 · 234 · 82 255 : 255 · 255 · 252 27 : 154 · 234 · 81 114 · 114 · 114 · 114 218 · 85 · 152 · 99 K. Cancel		16 Protocol S.,. IPv6 A.,. IPv6 Address/P.,. Down 1-1 records. Total: 1 records.   Show 10 ⊻
🔐 User Management					

#### ACL 设置(不然无法通讯)

C AR Web Platform x ← → C ▲ 不安全   bttp://www.sec.edu	\$://192.168.2.1/view/main/default.html?Version=1.2	&pageid=272136	A COLOR OF THE	_	★ * * :			
AR Web Plat	form			Current User: admin 🛛 🖫	🛿 Save 🥔 Help 🕕 About 🏂 Logout			
Pevice Information	Your Position : Security > ACL > Advanced ACL Setting							
🚍 Configuration Wizard	Basic ACL Setting Advanced ACL Setting Layer 2 ACL Setting Time Range							
중 LAN Access	Advanced ACL Setting List							
KAN Access	🕂 Create   🏐 Refresh							
IP Service	ACL	Type			Operation			
Security	Rule Number Source IP/Prefix Length(Wildcar	d) Destination IP/Prefix Length(Wildcard)	* Action * Protocol Typ	e Source Port	Add rules × Destination Port Operation			
ACL	5 192.168.2.0/0.0.255	192.168.1.0/0.0.255	Permit IP		Advanced 🔀			
Firewall	4 4   Page 1 of 1   ▶ ▶		Displaye	d: 1-1 records. Total: 1 record	Is.   Show 10 v records per page			
### IPsec 配置截图 1

IPSec connection name:	center_vpn		(1-12 characters)
Interface name:	Ethernet0/0/4		
Networking mode:	Branch site	) He	adquarters site
KE Parameter Setting			
IKE version:	v1	○ v2	
Negotiation mode:	Main mode	🔘 Ag	gressive mode
Authentication mode:	Pre-shared key	O RS.	A certificate
Pre-shared key:	1234	56	(1-127 characters)
Authentication algorithm:	MD5	*	
Encryption algorithm:	3DES	~	(The security level of this algorithm is low)
DH group number:	Group2	×	
DC D			
Psec Parameter Setting			
	ESP	*	
ESP autnentication algorithm:	MD5	*	
ESP encryption algorithm:	3DES	*	(The security level of this algorithm is low)
Encapsulation mode:	Tunnel mode	🔘 Tra	nsport mode
	ок с	ancel	
c	ОКС	ancel	
c 配置截图 2 fv IPSec Policy	ок с	ancel	
c 配置截图 2 ify IPSec Policy	ок с.	ancel	
c 配置截图 2 ify IPSec Policy ACL name:	OK C	ancel	
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫	OK C	ancel _1 ▼	
rc 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type:	OK C.	ancel _1 ▼ ● Na	me
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name:	OK C: C_Ethernet0/0/4 IP address DX3001	_1 ▼ ● Na	me (1-127 characters)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal:	OK C c_Ethernet0/0/4 ○ IP address DX3001 ⓒ Enabled	ancel _1 ✓ ● Na	me (1-127 characters)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection):	OK C.	_1 ¥	me (1-127 characters)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type:	OK C. C_Ethernet0/0/4. ● IP address DX3001 ● Enabled ● Enabled periodic	ancel _1 ▼ ● Na	me (1-127 characters)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets	OK C c_Ethernet0/0/4 IP address DX3001 Enabled Periodic seq-notify-hash	ancel _1 ♥ ● Na	me (1-127 characters)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds):	OK C.	_1 ▼ ● N:	me (1-127 characters) (10-3600, default value 30)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds)	OK C C_Ethernet0/0/4 ■ IP address DX3001 ■ Enabled ■ Enabled ■ Enabled periodic : seq-notify-hash 30 : 15	ancel _1 ▼ ● Na	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count:	OK C: c_Ethernet0/0/4, IP address DX3001 C Enabled Periodic Seq-notify-hash 30 15 3	ancel _1 ▼ ● Na	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 3)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server:	OK C C_Ethernet0/0/4 ■ IP address DX3001 ■ Enabled ■ Enabled ■ eriodic : seq-notify-hash 30 : 115 3 ■ Enabled	_1 ▼ ● N: ▼	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 3)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server: PFS:	OK C C_Ethernet0/0/4 ■ IP address DX3001 ■ Enabled ■ Enabled periodic : seq-notify-hash 30 : 15 3 ■ Enabled - none -	ancel _1 ▼ ● Na	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 3)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server: PFS: IKE SA lifetime (seconds):	OK C C_Ethernet0/0/4, IP address DX3001 Enabled Periodic Seq-notify-hash 30 15 3 Enabled - none - 86400	ancel _1 ✓ ● Na	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 3) (60-604800, default value 86400)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server: PFS: IKE SA lifetime (seconds): IPSec SA aging mode:	OK C. C_Ethernet0/0/4. IP address DX3001 ✓ Enabled ✓ Enabled ✓ eriodic : seq-notify-hash 30 : 115 3 — Enabled - none - 86400 Time-based (s) 3	ancel _1 ▼ ● N: ▼	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 3) (3-10, default value 3) (60-604800, default value 86400) (100-604800, default value 3600)
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server: PFS: IKE SA lifetime (seconds): IPSec SA aging mode:	OK C C_Ethernet0/0/4 ■ IP address DX3001 ■ Enabled ■ Enabled Periodic : seq-notify-hash 30 : 15 3 ■ Enabled - none - 86400 Time-based (s) 3 Traffic-based (KB)	ancel _1 ▼ ● Na ● Na • • • • • • • • • • • • • • • • • • •	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 15) (3-10, default value 3) (60-604800, default value 86400) (100-604800, default value 3600) 00 (0,2560-4194303, default value 184320
c 配置截图 2 ify IPSec Policy ACL name: Advanced ≫ Local identity type: Remote name: NAT traversal: DPD(Dead Peer Detection): DPD type: The sequence of the payload in DPD packets Idle time for DPD detection (seconds): DPD packet retransmission interval (seconds) DPD packet retransmission count: Enable Efficient VPN server: PFS: IKE SA lifetime (seconds): IPSec SA aging mode: Route import:	OK C C_Ethernet0/0/4 IP address DX3001 Enabled Finabled Periodic seq-notify-hash 30 15 3 Enabled - none - 86400 Time-based (s) 3 Traffic-based (KB) Enabled	ancel _1 ▼ ● Na ▼ 600 ) 18432	me (1-127 characters) (10-3600, default value 30) (3-30, default value 15) (3-10, default value 15) (3-10, default value 3) (60-604800, default value 86400) (100-604800, default value 86400) 00 (0,2560-4194303, default value 184320

# 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

	STATUS	NETWORK	FIREWALL	VPN
	Connecti	on Priority Set	ting the internet connection	nriority
Connection		ORK > Connection	I Priority	phoney
Cellular Link1				
Cellular Link2	III Conn	ection Priority		
WAN	Primary C Secondar	onnection v Connection	Cellular Link1 V WAN	
LAN	Tertiary C	onnection	Cellular Link2	
	Auto Dete	ect	Disable 💌	
		Save	Cancel	

配置 SIM1 的 APN 参数

# 福达新创通讯科技(厦门)有限公司 福达 VPN 产品使用手册

	Cellular Link1 Retrieve the	DNS server address from cellular network
Connection	🏦 NETWORK > Cellular Link1	
Cellular Link1		
Cellular Link2	≣ Cellular Link1	
WAN	Operator	Auto 💌
	User Name	
LAN	Password	
	APN	3gnet
	Authorization Mode	Auto 💌
	Dial-up Number	*99#(UMTS/3G/3.5G)
	Dial-up Mode	Always online 💙
	Redial Interval	30 (second)
	Redial Times	0 (0 means always redial)
	Max Idle Time	0 (0 means always online)
	Connection Check Interval	60 second (0 means not checked)
	Connection Check Times	5
	MTU	1492
		Save Cancel

设置 VR301 的 IPSec 参数

Device X		And a second sec				-
C 🛈 192.168.2.1	L/index.html?0.4371068407091	7893			17 20 ☆ 第 学	
ac	企 VPN > IPSec Settin	ng				
NVPN		-				
	IPSec Setting					
	Name:	DX3001	Enable:	Yes 🔹		
	IPSec Type:	Net-to-Net	IPSec Role:	Client		
	Local WAN Interface:	WAN .	Peer WAN Address:	27.154.234.82		
ificate	Local Subnet:	192.168.2.0 / 24	Peer Subnet:	192.168.1.0 / 24		
	Local ID:	@DX3001	Peer ID:	@Huawei		
Log						
	m Phasel					
	IKE Encryption:	3DES •	IKE Integrity:	MD5 •		
	IKE DH Group:	Group2(1024)	IKE Lifetime:	120 (120-86400sec.)		
	III Phase2					
	ESP Encryption:	3DES .	ESP Integrity:	MD5 •		
	PFS:	Disabled •	ESP Keylife:	120 (120-86400sec.)		
	III Advanced					
	Negotiation Mode:	Main Mode •	IP Compress:	Disabled •		
	DPD Detection:	Disabled •	Time Interval:	60 (Sec.)		
	Timeout:	60 (Sec.)	DPD Action:	Hold		
	I Authentication					
		100.000				
	Use A Pre-Shared Key	123456				

AR201 的 WAN 配置

## 福达新创通讯科技 (厦门)有限公司



#### ACL 设置

Web Plat	form				Current Use	n admin I	🗑 Save 🥔 Help 🕕	About 😗 Logi
Device Information	Your Position : Security > ACL > Advanced Basic ACL Setting Advanced ACL Setting	ACL Setting	ime Range					
CAN Access	Advanced ACL Setting List	Add Rules				×		
Z WAN Access	🖕 Create   💁 Refresh	Rule number:	5	(0-4294967294)				
WLAN AC	ACL	Action:	Permit     Only					Operation
1 ID Service	a Sternet0.0/l 1	<ul> <li>Protocol type:</li> </ul>	IP ¥					
2 - Garrier	Rule Number Source IP/Pretix	Matched priority:	- none - 💌				Destination Port	Operation
Security	5 192 168 1.0/0.0 (	ToS priority:		(0-15)				
AGL	If I Page 1 of 1 P PI	Matched IP Address					cords. Show 10 M	records per p
Firewall		Source IP address:	192 . 168 . 1 . 0	Wildcard:	0 .0 .0 .255			
802.1X Authentication		Destination IP address:	192 - 168 - 2 - 0	Wildcard:	0 . 0 . 0 . 255			
MAC Authentication								
Security Protection		Time range:	- none - 🛛 👻					
SSL								
PKI								
AAA								
Network Behavior Manaç								
Qos			OF	Cancel				
						_	R. Contraction of the second s	

### AR201 的 IPSec 配置 1

→ C ▲ 不安全 Ma	aps://192.168.1.1/view/main	n/default.html?Version=1.28pagei	d=362466	0	urrent User: admin 🛛 🗐 Save 🔗 Help	About Degou
P Device Information	Your Position : $VPN > IP$	Modify IPSec Policy			×	
Configuration Wizard	IPSec Policy Manageme	* IPSec connection name:	huawei	(1-12 characters)	Î	
LAN Access	IPSec Policy Managem	<ul> <li>Interface name:</li> <li>Networking mode:</li> </ul>	Ethernet0/0/8			
& WAN Access	Create X Delete	IKE Parameter Setting	Contraction and		Oneration	
WLAN AC	V huawei	IKE version:	● v1	© v2	B	
IP Service	14 4 Page 1 of	Negotiation mode:	Main mode	Aggressive mode	records Total 1 records.   Show 10	records per page
Security		Authentication mode:	Pre-shared key	RSA certificate		
QoS		Pre-shared key:		(1-127 characters)		
VPN	1	Encontion algorithm:	PIDS 20ES	(The accusts land of this electric is law)		
IPSec VPN	1	DH group number;	Group2	(The second rever of and adjoint in to ov)		
L2TP VPN						
SSL VPN		IPSec Parameter Setting				
VPN Instance		Security protocol:	ESP	*		
System Management		ESP authentication algorithm:	MD5	~		
User Management		ESP encryption algorithm: Encapsulation mode:	3DES Tunnel mode	Transport mode		
			(ок) с	ancel		

#### AR201 的 IPSec 配置 2

	tps://192.168.1.1/view/main	/default.html?Version=1.2&pageId=	362466#	☆ 赤 赤
AR Web Pla	tform	A Company	Cu	ment User: admin 🛛 🗐 Save 🛷 Help 🕐 About 🖓 Logout
	Your Poston : VPN - Difference Policy Managore Differe Policy Managore de Create : De Device IP Police Constant De Device De Device IP Police Constant De Device D	Indiffy IPSec Policy IPSec Policy IPSec Varanteer setting Security protocol: ESP exciption algorithm: EsP encipition algorithm: Encapalization mode: AdL name: Advanced s Local identity type: Remote name: NAT travensal: EPRIf fead Beer Execution):	ESP W HDS W 3DES W (The security level of this algorithm is low) Trunnel mode © Transport mode p_Etherneth/0/8_1 W DCIO01 (1-127 churachers) P Etherneth (0/8_1 W DCIO01 (1-127 churachers) P Etherneth (0/8_1 W Etherneth (0/8_1 W DCIO01 (1-127 churachers)) P Etherneth (0/8_1 W Etherneth (0/8_1 W) Etherneth (0/8_1 W Etherneth (0/8_1	X Operation Provide State
LITE VPN SBL VPN VPN Instance System Management User Management		Enable Efficient VPN server: PPS: JPE SA lifetime (seconds): JPSec SA aging mode: Route import: Pre-extraction of original IP packets:	Enabled     Finabled     Finabled     fone -     fine-based (s) <u>16660</u> (60-4800, 64fault value 86400)     Time-based (s) <u>16660</u> (100-40-4800, 64fault value 86400)     Tinffic-based (s) <u>1681200</u> (0.2560-1194303, 64fault value 1843200)     Enabled     Ork Cancel	

5.1.7 华为 AR151 与 VR301 的 L2TP 配置



### VR301 的设置通过 SIM1 来上网

	STATUS	NETWORK	FIREWALL	VPN
	Connection	n Priority Setti	ng the internet connection	n priority
Connection	☆ NETWOR	RK > Connection	Priority	
Cellular Link1			-	
Cellular Link2	🗏 Conne	ction Priority		
WAN	Primary Co	nnection	Cellular Link1 💙 WAN	
LAN	Secondary Tertiary Cor	nection	Cellular Link1 Cellular Link2	
	Auto Detect	t	Disable	
		Save	Cancel	

配置 SIM1 的 APN 参数

# 福达新创通讯科技(厦门)有限公司 福达 VPN 产品使用手册

	Cellular Link1 Retrieve the	DNS server address from cellular network
Connection	🏦 NETWORK > Cellular Link1	
Cellular Link1		
Cellular Link2	🗮 Cellular Link1	
WAN	Operator	Auto 💌
	User Name	
LAN	Password	
	APN	3gnet
	Authorization Mode	Auto 💌
	Dial-up Number	*99#(UMTS/3G/3.5G)
	Dial-up Mode	Always online 💙
	Redial Interval	30 (second)
	Redial Times	0 (0 means always redial)
	Max Idle Time	0 (0 means always online)
	Connection Check Interval	60 second (0 means not checked)
	Connection Check Times	5
	MTU	1492
		Save Cancel
		Califer

## VR301 的 L2TP 的配置

IADevice ×			
C ① 不安全   192.168.2.1/index.html	20.43710684070917893		距☆ 奔
Sec ( VPN > 1	210		
enVPN			
II Basic S	ettings		
L2TP Mode	Client •		
L2TP Server	27.154.234.82		
E User Name	huawei		
rtificate Password		Unmask	
Obtain IP	Auto 🔻		
N Log IP Address	192.168.33.254		
Subnet Mask	255.255.255.255		
Gateway	192.168.33.7		
DNS	172.17.92.114		
Authorization	Mode Auto *		
MPPE	Disabled •		
NAT	Disabled •		
MTU	1460	(576-1460)	
Connection (	heck Interval 60	Sec(0 means not checked)	
Connection 0	heck Times 5		
IPSec Encryp	tion Disable	ंग	
Connection S	tatus Connected		

AR151 的 WAN 口设置

# 福达新创通讯科技(厦门)有限公司

mailleaff	愈的位置:广域网互联 > 修	改以太接口		×		
ECUIDI-F		描述:	HUAWEI, AR Series, Ethe (1~242个字符)	-		
局域网接入	以入接口	元/电接口: 当前中口描:	电			
广域网互联	以太接口列表	自协商:	··· ● 伸能 □ 未伸能			
(1) - 1473	搜索项: 接口名称					
	- ●新建   > 開除   警号	✓ IPv4 ▼				
Dougen	□ 接口名称 接	接入方式:	◎ DHCP 配置从ISP处自动获得IP地址	>v	6协议状态 IPv6 IPv6	地址/前缀 操作
	Ethernet0/0/4 HL		Static 配置从ISP处装得的固定评地址		不可用	
SA掇口	第1页共	· ID-Mainh ·	● PPPOE 副金元ISP2C银信的用户省及密码		当前显示第1到1条记录/	共1条记录 每页 10 🖌
CE1/CT1接口	1		27 . 154 . 234 . 82			
E1/T1接口		*子网摘码:	255 . 255 . 255 . 252			
PON接口		默认网关:	27 . 154 . 234 . 81			
芝辑接口		首诀DNS服务器:	114 . 114 . 114 . 114			
接口备份		A BONCOPA No.				
叩业务		南田山へて	218 . 65 . 152 . 99			
		启用INA 1.	●是 ◎召	•		
安全			确定取消			

### AR151 的 L2TP 配置

(读 设备数)	您的位置: VPN > L2TP VPN >	修改L2TP服务器	×					
<ul> <li>■ 配置向导</li> <li>■ 局域网接入</li> <li>20 广域网互联</li> </ul>	<ul> <li>① 开启に2TP客户端和L2TP服务</li> <li>全局配置</li> <li>L2TP功能: ●开启 ○ 关注</li> </ul>	<mark>建道成置</mark> 默认服道: ◎ 井倉 随道认证: □ 开倉						
<ul> <li>□ □业务</li> <li>♥ 安全</li> </ul>	L2TP寄户端 L2TP服务表 服务器列表 中新建 X 物称 D 年白 1	* i认已方式: ● PAP ◎ CHAP AAA城: -none - M						
QoS VPN IPSec VPN	<ul> <li>☑ 釐遊名称</li> <li>☑ 默认隧道</li> <li>Ⅰ 4 1 第 1 页共1页</li> </ul>	<b>地址分配设置</b> - 同关护/于网模码: 192.168.33 .7 / 255.255.25		前显示第	1到1茶记录/-	一共1条记录	1 卷页 10	▼ 条
L2TP VPN SSL VPN VPN实例		高級 ※ 勝勢器名称: Huawel (1~30个字符) 保酒時間(地): 60 (0~1000.意认值=60)						
系统管理 用户管理		AVP数据: 隐羅 强制LCP重协商: 开启 强制CHAP认证: 开启						

## AR151 新新建一个用户可以通过 PPP 类型进行接入

一 设备数约	您的位置: 用户管理					
🛄 配置向导	用户管理					
臺 局域网接入	用户列表	修改用户		×		
名 广域网互联 III P业务	<ul> <li>◆ 新連   × 前級   ⑤ 刷新</li> <li>○ 用户名称</li> <li>○ admin</li> </ul>	* 用户名: 新密码:	huawei	(1~64个字符) (8~128个字符)	授作	
💙 安全	V huawei	确认密码:	••••••	]		
<ul> <li>QoS</li> <li>VPN</li> <li>系统管理</li> </ul>	( 第 1 页共1页  >	<ul> <li>○ 访问级别:</li> <li>● 接入类型:</li> </ul>	<ul> <li>普通管理员</li> <li>所有</li> <li>http</li> <li>web</li> <li>ftp</li> <li>telnet</li> <li>bind</li> <li>termina</li> </ul>	ssh 802.1x	当前显示第1到2件记录/一共2条记录 每页	į 10 🗸
用户管理用户管理			Ø ppp ↓ x25-pai 确定 取消			

# 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

	STATUS NETWORK	FIRE <b>WALL</b>
Connection	WAN configure internet o	connection
Cellular Link1 Cellular Link2	I WAN Settings	
WAN	WAN Mode	STATIC •
LAN	IP Allocation Method	Manual 🔻
	IP Address	10.0.0.1
	Network Mask	255.255.255.0
	Gateway Address	10.0.0.2
	Packet MTU	1500
	(Don't change the settings	s unless really need to)
	Retrieve DNS Address By:	Manual 💌
	Primary DNS	114.114.114.114
	Secondary DNS	114.114.114.118

VR301 的 IPSec 配置

# 福达新创通讯科技(厦门)有限公司

福达 い	VPN	产	品作	吏用	手	册
------	-----	---	----	----	---	---

	IPSec Type:	Net-to-Net *	IPSec Role:	Client •
	Local WAN Interface:	WAN •	Peer WAN Address:	10.0.0.2
ate	Local Subnet:	192.168.1.0 / 24	Peer Subnet:	192.168.2.0 / 24
	Local ID:	10.0.0 1	Peer ID:	10.0.0.2
1	III Phase1			
	IKE Encryption:	3DES •	IKE Integrity:	MD5.
	IKE DH Group:	Group2(1024)	IKE Lifetime:	120 (120-86400sec.)
	PFS:	Disabled •	ESP Keylife:	120 (120-86400sec.)
	⊞ Phase2			
	PFS:	Disabled	ESP Keylife;	120 (120-86400sec.)
	I Advanced	1	Transfer .	
	Negotiation Mode:	Main Mode •	IP Compress:	Disabled •
	DPD Detection:	Enabled	Time Interval:	60 (Sec.)
	Timeout:	60 (Sec.)	DPD Action:	Hold •
	=			
	# Authentication			
	<ul> <li>Authentication</li> <li>Use A Pre-Shared Key:</li> </ul>	Delta123		
	<ul> <li>Use A Pre-Shared Key:</li> <li>Use The X.509 Cert:</li> </ul>	Delta123		
	Use A Pre-Shared Key: Use The X.509 Cert:	Delta123		

思科 RV130W 的 WAN 口配置

ı اسال Small Busines دىsco RV130W	s Wireless-N VPN I	Firew	/all			
Getting Started <ul> <li>Status</li> </ul>	WAN Configuration					
* Networking	Internet Connection Type:	Static	IP		•	]
► WAN	Static IP Settings					
MAC Address Clone Routing	Internet IP Address:	10	.0	.0	.2	(Hint: 192.168.100.100)
Routing Table	Subnet Mask:	255	. 255	.255	.0	(Hint: 255.255.255.0)
Dynamic DNS IP Mode	Default Gateway:	10	.0	.0	100	(Hint 192.168.100.1)
▶ IPv6	DNS Server Source:	Use these DNS Servers 🔻				
Wireless	Static DNS 1:	114	. 114	. 144	. 114	(Hint: 1.2.3.4)
Firewall	Static DNS 2:	8	.8	.8	.8	1
VPN	Ontional Sottings				- Ale	
Administration	MTU:	Aut	o 🔘 Man	ual		
7	Size.	1500			Bytes (F	Range: 576 - 1500. Default: 150

思科 RV130W 的 IPSec 配置 1

# 福达新创通讯科技(厦门)有限公司

Small Busines	s Wireless-N VDN	Firewall	
Setting Started		riicwali	
tatue	Add / Edit IKE Policy Con	figuration	
Intuoting	IKE Name:	test	
Nireless	Exchange Mode:	Main 🔻	
Vireiess	Local		
rewan	Local Identifier Type:	IP Address 🔹	
IPN	Local Identifier:	10.0.0.2	
Resic VPN Setup	Remote		
Advanced VPN Setup	Remote Identifier Type:	IP Address 🔹	
PSec VPN Server	Remote Identifier:	10.0.0.1	
PTP Server	IKE SA Parameters		
oS	Encryption Algorithm:	3DES 🔻	
dministration	Authentication Algorithm:	MD5 T	
	Pre-Shared Key:	Delta123	
	DH Group:	Group2 (1024 bit) 🔻	
	SA-Lifetime:	28800	Seconds (Range: 30 - 86400, Default: 28800)
	Dead Peer Detection:	Enable	
	DPD Delay:	10	(Range: 10 - 999, Default 10)
	DPD Timoout	20	(Range 20, 1000 Default 20)

## 思科 RV130W 的 IPSec 配置截图 2

Getting Started	Advanced VPN Setup		
* Status	-		
Networking	Add / Edit VPN Policy Configu	iration	
Wireless	IPSec Name:	DX3001	
Firewall	Policy Type:	Auto Policy 🔹	
* VPN	Remote Endpoint	IP Address V	
<ul> <li>Site-to-Site IPSec VPN</li> <li>Basic VPN Setup</li> </ul>		10.0.0.1	(Hint: 1.2.3.4 or abc.com
Advanced VPN Setup	NetBios Enabled:		
IPSec VPN Server	Local Traffic Selection		
VPN Passthrough	Local IP:	Subnet 🔻	
• QoS	IP Address:	192.168.2.0	(Hint: 1.2.3.4)
Administration	Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)
	Remote Traffic Selection		
	Remote IP:	Subnet •	
	IP Address:	192.168.1.0	(Hint: 1.2.3.4)
	Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)
	Manual Policy Parameters		
	SPI-Incoming:	0x	
	SPI-Outgoing:	0x	
	Manual Encryption Algorithm:	3DES V	

#### 思科 RV130W 的 IPSec 配置截图 3

Manual Encryption Algorithm:	3DES 🔻	
Key-In:		
Key-Out:		
Manual Integrity Algorithm:	SHA-1 V	
Key-In:		
Key-Out:	1	
Auto Policy Parameters		
IPSec SA Lifetime:	3600	Seconds (Range: 30 - 86400, Default 3600)
Encryption Algorithm:	3DES T	
Integrity Algorithm:	MD5 T	
PFS Key Group:	C Enable	
DH Group:	Group 1(768 bit) 🔻	
Select IKE Policy:	test •	
	Mew	
Save Cancel	Back	

# 5.2.2 思科 RV325 与 VR301 的 IPSec(PSK)配置



VR301 的设置通过 SIM1 来上网

	STATUS	NETWORK	FIREWALL	VPN
Connection	Connecti	on Priority Set	ing the internet connection	priority
Cellular Link1	☆ NETW	ORK > Connection	Priority	
Cellular Link2 WAN	III Conn Primary C	ection Priority onnection	Cellular Link1 🗸	
LAN	Secondar Tertiary C	y Connection onnection	Cellular Link1 Cellular Link2	
	Auto Dete	ect	Uisable Y	
		Save	Cancel	

## 配置 SIM1 的 APN 参数

	Cellular Link1 Retrieve the (	DNS server address from cellular network
Connection	⚠ NETWORK > Cellular Link1	
Cellular Link1		
Cellular Link2	🗏 Cellular Link1	
WAN	Operator	Auto 💌
	User Name	
LAN	Password	
	APN	3gnet
	Authorization Mode	Auto 🔽
	Dial-up Number	*99#(UMTS/3G/3.5G)
	Dial-up Mode	Always online 💙
	Redial Interval	30 (second)
	Redial Times	0 (0 means always redial)
	Max Idle Time	0 (0 means always online)
	Connection Check Interval	60 second (0 means not checked)
	Connection Check Times	5
	MTU	1492
		Cause
		Save Cancer

VR301 的 IPSec 配置

DIADevice ×				
→ C ① 192.168.1.1/index.h	ntml70.827737693345186	1		
	VPN Setting IPSec Se	tting		
IPSec	☆ VPN > IPSec Setting			
OpenVPN	9			
	■ 1PSec Setting			
PARTIN.	512 mar a t	DV336	-	Vee
L2TP	Name:	Ny J20	Enable:	res •
GRE	IPSec Type:	Masi .	Dese Wate Address	07 154 234 166
anaza Articar (alter	Local WAN Interface:	192 168 1 0 / 24	Peer wan address:	AC 1 0 C R3F C0F
Certificate	Local Subnet:	@DX3001	Peer Subnet:	(152.100.2.0 / 24
/PN Log	Local ID;	@DX3001	Peer ID:	(Brisco
	🗏 Phasel			
	IKE Encryption:	3DES •	IKE Integrity:	MD5 •
	IKE DH Group:	Group2(1024)	IKE Lifetime:	28800 (120-86400sec.)
	⊞ Phase2			
	ESP Encryption:	3DES •	ESP Integrity:	MD5 •
	PES:	Disabled •	ESP Keylife:	3600 (120-86400sec.)
	2012012			
	I Advanced			
	Negotiation Mode:	Aggressive Mode	IP Compress:	Disabled •
	DPD Detection:	Enabled •	Time Interval:	50 (Sec.)
	Timeout:	60 (Sec.)	DPD Action:	Hold
		410 80		
	I Authentication			
	Lico A Dro Chanad Kaus	Delta123		
35的WAN口配置 Cisco RV325 Configure × → C ▲ 不安全 □ bttps:	//192.168.2.1/default.h			
Setting Started	DIT DUAI WAN V	PN Router		
system Summary	Network			
ietup Notwork	WAN Connection Settings			
Password	Interface:	WAN1		
Time DM7 Host	WAN Connection Type:	Static IP	•	
Forwarding	Specify WAN IP Address:	27.154.234.166		
Port Address Translation	Subnet Mask:	255.255.255.252		
MAC Address Clone	Default Gateway Address:	27.154.234.165		
Dynamic DNS	DNS Server 1:	218.85.152.99		
Inbound Load Balance	DNS Server 2:	218.85.157.99		
USB Device Undate	MTU:	Auto Ma	nual 1500 B (Ra	inge:68~1500, Default:1500)

RV235 的 IPSec 配置截图 1

USB Device Update

• DHCP System Management

Save Cancel Back

👑 Cisco RV325 Configure >		
← → C ▲ 不安全   Þ	Hps://192.168.2.1/default.htm	
CISCO RV325 G	igabit Dual WAN VPN F	Router
Getting Started	Add a New Tunnel	
System Summary	Tunnel No.	1
<ul> <li>Setup</li> </ul>	Tunnel Name:	DX3001
▶ DHCP	Interface:	WAN1
<ul> <li>System Management</li> </ul>		
<ul> <li>Port Management</li> </ul>	Keying Mode:	IKE with Preshared key
Firewall	Enable:	2
Summary Gateway to Gateway Client to Gateway VPN Passthrough PPTP Server	Local Group Setup Local Security Gateway Type: IP Address:	IP + Domain Name(FQDN) Authentication
Certificate Management	Domain Name:	CISCO
▶ Log	Local Security Group Type:	Subnet •
SSL VPN	IP Address:	192.168.2.0
User Management	Subnet Mask:	255,255,255,0
Wizard		
	Remote Group Setup Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
	Domain Name:	DX3001
	Remote Security Group Type:	Subnet
	IP Address:	192.168.1.0
	Subnet Mask:	255.255.255.0

### RV235 的 IPSec 配置截图 2

Phase 1 DH Group:	Group 2 - 1024 bit	•
Phase 1 Encryption:	3DES	T
Phase 1 Authentication:	MD5	▼
Phase 1 SA Lifetime:	28800	sec ( Range: 120-86400, Default: 28800
Perfect Forward Secrecy:		
Phase 2 Encryption:	3DES	T
Phase 2 Authentication:	MD5	T
Phase 2 SA Lifetime:	3600	sec ( Range: 120-28800, Default: 3600 )
Minimum Preshared Key Complexity:	Enable	
Preshared Key:	Delta123	
Preshared Key Strength Meter:		

RV235 的 IPSec 配置截图 3

Ad	110	ne	od	
AU	٧d	nc	eu	1

Advanced		
Aggressive Mode		
Compress (Support IP Payload	d Compression Protocol(IPCom	0))
Keep-Alive		
AH Hash Algorithm MD5 •		
NetBIOS Broadcast		
Multicast Passthrough		
🕑 NAT Traversal		
Dead Peer Detection Interval	10 sec ( Range: 10-999,	Default 10 )
Extended Authentication:		
IPSec Host		
User Name:		ſ
Password:	J	
Edge Device	Default - Local Database 🔻	Add/Edit
🔲 Tunnel Backup		
Remote Backup IP Address:		Name or IPv4 Address
Local Interface:	WAN1	
VPN Tunnel Backup Idle Time:	30	sec ( Range: 30-999, Default: 30 )

# 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

## 福达新创通讯科技(厦门)有限公司

	STATUS	NETWO	DRK	FIREWAL	L VPI
	Connecti	ion Priority	Setting	the internet co	nnection priorit
Connection		/ORK > Conn	ection Pri	ority	interesteri priorie
Cellular Link1					
Cellular Link2	II Conn	ection Prio	rity		
WAN	Primary C Secondar	Connection		Cellular Link1	~
LAN	Tertiary C	Connection		Cellular Link1 Cellular Link2	
	Auto Dete	ect		Disable 🔽	
		Sa	we	Cancel	

VR301 的 SIM1 的 APN 参数设置

_____

	Cellular Link1 Retrieve the	DNS server address from cellular network
Connection	🏦 NETWORK > Cellular Link1	
Cellular Link1		
Cellular Link2	≣ Cellular Link1	
MAN	Operator	Auto 💌
	User Name	
LAN	Password	
	APN	3gnet
	Authorization Mode	Auto 💌
	Dial-up Number	*99#(UMTS/3G/3.5G)
	Dial-up Mode	Always online
	Redial Interval	30 (second)
	Redial Times	0 (0 means always redial)
	Max Idle Time	0 (0 means always online)
	Connection Check Interval	60 second (0 means not checked)
	Connection Check Times	5
	MTU	1492
		Save Cancel

VR301 的 VPN 证书导入

IPSec	VPN Setting Certificate				
OpenVDN	☆ VPN > Certificate Mana	gement			
	🗮 Certificate Managem	ent			
РРТР	Group Name	Cert Pass	word		
L2TP	Import CA	coCort nom		coCort no	
GRE	Import CA	Lacerupem	(刈丸	cacert.pe	
Certificate	Import Public Cert	clientCert.pem	浏览	clientCert	
VPN Log	Import Private Key	clientKey.pem 1234	56 浏览	clientKey.j	
		, 			
	Import Peer Public Cert	serverCert.pem	浏览	serverCer	
	Import CRL		浏览		
		Save	Cancel		
导入后显示如一	۲:				
	🗏 Connection Man	agement			
РРТР					
L2TP	Group Name	e CA Public Cer	t Private Cert	Expired Date	Operation
GRE	Cert	caCert.pe clientCert.p m m	e clientKey.pem	2018-Mar- 30/07:03:01/GMT	Edit   Download   Delete
Certificate					
NDN Log			Add		
VB301的的IPS	ec 配置				
IPSec Setting					
Name:	Test	ahla	Yes	*	
IDSec Type:	Net-to-Net	Sec Role:	Client	~	
Local WAN Interface:	WAN Pe	er WAN Address	27, 154, 234, 82		
Local Subpati		r Subpot	192 168 0.0	1 24	
Local Subnet.	apy2001	r subriet.	asc1000	7 27	
Local ID:	90X3001 P8	Br 1D:	@PG1000		
≣ Phase1					
IKE Encryption:	3DES VIKE	Integrity:	MD5	~	
IKE DH Group:	Group2(1024)	Lifetime:	120 (120-8	6400sec.)	
ine off of oup.		Liotino	(120 0		
≣ Phase2					
ECD Encruption	3DES		MD5		
ese encryption:	Enabled	- megney:	120 /100.0	(6400ccc)	
	Croup2(1024)	- value:	120 (120-8	0400580.)	
OH Group:					
⊞ Advanced					
Negotiation Mode	Main Mode	Compress:	Enabled	~	
DPD Detection:	Enabled V Tim	e Interval:	60 (Sec.)		
Timeout:	60 (Sec.) D0	D Action:	Hold	*	
nneouc.	(380.) DP		1.1010		
Authentication					
Use A Pre-Shared Key:					
I Use The X.509 Cert:	Cert •				
		AddCaped			
		Add Cancel			

### FG100D 的 WAN 口配置

系统管理		编辑接口
● ② 仪表板 ● ● 秋恋 ● ● FortiView ● ⊇ 网络	接口名称 别名 连接状态 类型	wan1(90:6C:AC:32:26:F0) ╞ortiGate100D.wan1 已启用
	地址模式 IP/网络掩码	<ul> <li>● 自定义 ○ DHCP ○ PPPoE ○ Dedicated to FortiAP</li> <li>27.154.234.82/255.255.255.255</li> </ul>
<ul> <li>● 配置</li> <li>● ● 配置</li> <li>● ● 10 位书</li> <li>● ● 监视</li> </ul>	管理访问	ビ HTTPS ビ PING ビ HTTP ビ FMG-Access CAPWAP ビ SSH SNMP FCT-Access ビ 自动IPsec请求
	DHCP 服务器	□ 启用
	安全模式	无
	设备管理 检测并识别设备	
	监听 RADIUS 账单消息 附加的IP地址	
路由 筆略 8: 对象	· 注释 - 管理状态	:] 0/255

## FG100D的 IPSec 配置截图 1

系统管理	VPN创建向导
路由	
策略 & 对象	1 VPN Setup
安全配置文件	用户名
虚拟专网	模板
Psec	₩ 拨号 - FortiClient (Windows, Mac OS, Android)
·····································	🔀 Site to Site - FortiGate
■ 隧道模板	□ 拨号 - iOS (本地)
● <u>4</u> SSL ● ■ 些初発	接号 - Android (本地 L2TP/IPsec)
	■ 拨号 - Cisco 防火墙
	📓 Site to Site - Cisco
	自定义VPN 隧道(无模板)
	<返回 万一个> 取消

### FG100D的 IPSec 配置截图 1

	编辑 VPN 隧道	
用户名 注释	ipsec_test 10000 concurrent user(s) will be supported 注释	
网络		✓ ×
IP 版本	IPv4	
远程网关	拨号用户    ▼	
接口	wan1 (FortiGate100D.wan1)	
模式配置		
NAT穿越		
保持存活频率	10	
对等体状态探测		

FG100D 的 IPSec 配置截图 2

认证			<ul><li>✓ ×</li></ul>
方法	特征	•	
证书名称	ServerCert	- 0	
IKE			
版本			
Mode	○ Aggressive ⊙ 主模式(ID保护)		
对等体选项			
访问类型	任意对端 ID	•	

### FG100D的 IPSec 配置截图 3

Phase 1 Pi	oposal		③ 添加	✓ ×
加密	3DES	<ul> <li>认证</li> </ul>	1D5 •	
Diffie-Hellma	an 组	21 20 15 14	] 19 📄 18 📄 17 📄 16 ] 5 🕑 2 📄 1	
密钥生存时间	(秒)	86400	\$	
本地ID		FG100D		

FG100D的 IPSec 配置截图 4

用尸名	本地地址	Remote Address	
ipsec_test	192.168.0.0/255.255.255.0	192.168.2.0/255.255.255.0	
			17
编辑 Phase 2			
用户名	ipsec_test		
注释	注释		
本地地址	子网 192.	168.0.0/255.255.255.0	
Remote Address	子网 192.	168.2.0/255.255.255.0	
Advanced			
Phase 2 Proposal		💿 添加	
加密 3DE	3 🔹 认证 🛛 MD5	•	
启用重播检测 🗹			
启用完全前向保密 (PFS	i) 🗹		
Diffie-Hellman 组			
本地端口	全部 🗹		
	全部 🗹		
Remote Port			
Remote Port 协议	全部 🗹		
Remote Port 协议 自动密钥保持存活	全部 ☑ □		
Remote Port 协议 自动密钥保持存活 密钥周期(秒/kb)	全部 🔽 □ 秒	•	
Remote Port 协议 自动密钥保持存活 密钥周期(秒/kb) 秒	全部 ☑ □ 秒 43200	•	

# 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:

- 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
НМІ	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

- (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。