

PPTP 服务器配置:

1. 进入“计费认证/PPP 认证”中设置配置基本 PPP 服务，并开启

基本设置

运行服务 PPPoE服务 PPTP服务 L2TP服务

认证加密 PAP CHAP MS-CHAP v1 MS-CHAP v2

MPPE 拒绝加密

默认网关 192.168.65.178

允许远程拨入IP

分配地址池 192.168.65.1/24

DNS服务器 223.5.5.5

114.114.114.114

日志格式 摘要

免认证模式 启用 禁用

同一账户允许多用户在线 允许 (默认)

流量控制 启用 禁用

* 仅使用PPPoE服务，建议关闭MS-ChAPv1/v2

* 仅使用PPPoE服务，建议关闭MPPE加密

* 为空时远程地址和分配地址冲突，可能引起系统故障

* 仅PPTP/L2TP有效，有效格式：
• 网络: A.B.C.D/M 例如: 192.168.0.0/24
• 范围: A.B.C.D-M 例如: 192.168.0.1-255
• 为空则允许所有地址访问

* 需要重启服务，有效地址格式：
• 网络: A.B.C.D/M[name=poolname] 例如: 192.168.0.0/24
• 范围: A.B.C.D/M[name=poolname] 例如: 192.168.0.1-255,name=MyName

* 启用后不进行用户名密码认证

* 如需用户限速必须启用

2. 禁用免认证模式时需要在“计费认证/账户管理—用户管理”中添加账号密码

用户组管理 用户管理 优惠券管理 充值卡管理

刷新 + 添加 全部清除

帐号/名称/备注 全部状态 全部时间 帐号类型 全部认证类型 查询 导入 导出

ID	帐号	用户姓名	帐号类型	用户组	到期时间	状态	备注	启用	操作
1	111		全部	123	永不过期	正常		<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

全部启用 全部禁用

3. 在“计费认证/PPP 认证/在线用户”中查看在线情况

计费认证 / PPP认证 / 在线用户

基本设置 在线用户 历史流量 账号日志查询 PPPoE统计 L2TP会话

刷新 查询 全部清除 自服务状态

已连接/正在连接/已结束: 1/0/0

PPPT

ID	用户	IP地址	Caller ID	接口	流量(下行/上行)	限速下行/上行(Kb/s)	状态	在线时间	操作
1	112	192.168.11.2	192.168.2.138	-	0.0Kb/0.0Kb	-	已连接	00:00:05	<input type="checkbox"/>

1条记录 1/1 页

OPENVPN 配置:

1. 进入“网络安全/VPN/OPENVPN 客户端”中配置

编辑第1条SSLVPN隧道

名称	sslvpn1	*eg. 以sslvpn开头, 如sslvpn0, sslvpn1
服务器地址	103.244.1	*eg. 有效格式 192.168.0.1 [port]
接口类型	网络层	
协议	UDP	
服务证书	<input type="button" value="选择文件"/> 未选择任何文件	*文件已上传 .crt格式
HTTP代理服务器		*eg. 有效格式 192.168.0.1 [port]
用户名	smart6	
密码		
加密算法	AES	
	<input checked="" type="checkbox"/> 加载远端指定路由	
	<input type="checkbox"/> 启用数据压缩	
	<input type="checkbox"/> 强制服务器名称解析	
	<input type="checkbox"/> 开机自动连接	
	<input checked="" type="button" value="确定"/> <input type="button" value="取消"/>	

正确填写各参数，上传有效服务证书
连接后可在静态路由中看到如下路由

9	-	系统	192.168.150.0	255.255.255.0	192.168.150.101	sslvpn1	-	激活	-
10	-	系统	192.168.150.101	255.255.255.255		sslvpn1	-	激活	-

2. 在“网络安全/地址转换”中添加 VPN 相关规则

编辑第 '2' 条规则

来源地址	<input checked="" type="radio"/>	新地址项	A.B.C.D/M 或 A.B.C.D-A.B.C.D	<input type="checkbox"/> 来源地址取反 * 内网ip
	<input type="radio"/>	地址对象	CERNET	<input type="button" value="+ 添加地址对象分组"/>
指定目的	<input checked="" type="radio"/>	新地址项	192.168.150.0/24 本端获得地址网段	<input type="checkbox"/> 目的地址取反
	<input type="radio"/>	地址对象	CERNET	<input type="button" value="+ 添加地址对象分组"/>
端口对象		any		* 仅对匹配该对象数据做映射
出接口		sslvpn1		* 数据包从此接口出
随机分类				* 百分比, 有效值为0-100
报文标记				<input type="checkbox"/> 取反
转换地址类型	<input type="radio"/> 主机 <input type="radio"/> 网络 <input type="radio"/> 范围 <input checked="" type="radio"/> 地址伪装 <input type="radio"/> 仅通过 <input type="radio"/> 仅拦截			
转换后地址				* 公网IP, 如: 192.168.0.1, 192.168.0.0
转换后端口				* 转换指定端口, 如: 80, 135-139
备注				
		<input checked="" type="button" value="确定"/> <input type="button" value="取消"/>		

3.如果本机线路需要走 VPN 线路时，可做如下设置

①在“报文标记”中做线路标记规则

编辑第'1条'报文标记策略

来源地址	<input checked="" type="radio"/>	新地址项	0.0.0.0/0	<input type="checkbox"/>	来源地址取反
	<input type="radio"/>	地址对象	CERNET	<input type="button" value="+ 添加地址对象分组"/>	
目的地址	<input checked="" type="radio"/>	新地址项	0.0.0.0/0	<input type="checkbox"/>	目的地址取反
	<input type="radio"/>	地址对象	CERNET	<input type="button" value="+ 添加地址对象分组"/>	
端口对象	<input checked="" type="radio"/>	选择服务	any		
	<input type="radio"/>	自定义协议	TCP	<input type="text" value="端口"/>	
时间对象		任意			
入口		LAN1		<input checked="" type="checkbox"/>	*数据包从此接口入
更多高级选项	<input type="checkbox"/>	启用			

动作 报文标记 修改TCPMSS DSCP 自定义分组 通过

标记值 * eg. 100, 有效值为1-1000

备注

②做“静态路由”或者“策略路由”规则

静态路由：

新增静态路由项

类型	<input type="radio"/> 主机 <input checked="" type="radio"/> 网络	
目的地址	<input type="text"/>	* eg.
子网掩码	<input type="text"/>	* 默认
网关地址	<input type="text"/>	* eg.
接口	sslvpn1	* 可忽
优先级	<input type="text"/>	* 有效
报文标记	100	* 关,请使
路由探测	不探测	* 引用

策略路由：

路由规则 路由表

刷新 + 添加

显示数量：20条

ID	优先级
1	20000

共 1 条记录

编辑路由策略项1

优先级: 20000 *1 - 20000, 值越小, 优先级越高

来源地址: 0.0.0.0/0 *A.B.C.D or A.B.C.D/M

目的地址:

报文标记: 100 *引用数据流对象中定义的标记

服务类型: 0 *TOS/DSCP字段

接口: LAN1 *入接口

策略路由表: slvpn

确定 取消

路由规则 路由表

刷新 + 添加 全部清除 返回

显示数量：20条

搜索

ID	类型	目的地址	本地出口地址	优先级	服务质量	报文标记	网关	输出设备	状态	操作
1	-	0.0.0.0/0	-	0	0x0			slvpn1	激活	<input checked="" type="checkbox"/> <input type="checkbox"/>

共 1 条记录

← 上一页 1 下一页

IPSEC 配置:

1.进入“网络安全/VPN/--IPSEC”中配置

编辑IPSEC连接 'IPSEC'

隧道名称	IPSEC	* 由字母、数字和下划线组成,且不能以下划线开头
本地网关	192.168.2.138 本机外网IP	* 由IP地址或IP地址:端口组成
本地网络地址	192.168.65.0/24 本机内网网段	* 有效地址前缀:192.168.1.0/24
对端网关	192.168.2.169 对端外网IP	* 由IP地址或IP地址:端口组成
对端网络地址	192.168.111.0/24 对端内网网段	* 有效地址前缀:192.168.1.0/24

第一阶段设置

第二阶段设置

第一阶段设置

本地标识	IP地址	192.168.2.138 本机外网IP	
对端标识	IP地址	192.168.2.169 对端外网IP	
密钥交换模式	主模式		* 至少勾选一种交换模式
IKE密钥生存时间	3600	sec	* 只能输入整数,可以为空
验证方式	预共享	123456	* 只能输入整数,可以为空
加密算法	AES		
哈希算法	MD5		
DH分组	DH1		
更多高级设置	<input checked="" type="checkbox"/>	启用	
验证对端标识	<input checked="" type="radio"/>	启用	<input type="radio"/> 禁用
被动模式	<input type="radio"/>	启用	<input checked="" type="radio"/> 禁用
对应存活检测	<input type="radio"/>	启用	<input checked="" type="radio"/> 禁用
检测间隔			* 当“对应存活检测”启用时有效,有效值为 0-60 整数
最大重试次数			* 当“对应存活检测”启用时有效,有效值为 0-60 整数
检测延迟			* 当“对应存活检测”启用时有效,有效值为 0-60 整数
NAT穿越	启用		

第二阶段设置

封装协议	ESP		
数据传输模式	隧道模式		
生存时间	3600	sec	* 只能输入整数,可以为空
应用协议	所有		
加密算法	AES		* 至少勾选一种加密算法
验证算法	hmac_md5		* 至少勾选一种验证算法
压缩算法	IPComp		

设置好后开启服务并连接 PS:俩边参数需设一致

2.添加“静态路由”

新增静态路由项

类型 主机 网络

目的地址 对方内网网段 * eg. 192.168

子网掩码 * 默认值. 255

网关地址 * eg. 192.168

接口 本机外网口 * 可忽略, 系

优先级 * 有效值: 0 - 关,请使用不同的

报文标记 * 引用报文标记

路由探测

3.添加“地址转换”规则: 此规则需要放在最前面, 以免地址被其余规则优先转换, 使得此规则失效, 且本规则是走纯路由模式, 不影响其余规则

新增地址转换规则

来源地址 新地址项 地址对象

新地址项 来源地址取反 * 内网ip

地址对象

指定目的 新地址项 地址对象

新地址项 对端内网网段 目的地址取反

地址对象

端口对象 * 仅对匹配该对象数据做映射

出接口 * 数据包从此接口出

随机分类 * 百分比. 有效值为0-100

报文标记 取反

转换地址类型 主机 网络 范围 地址伪装 **仅通过** 仅拦截

转换后地址 * 公网IP, 如: 192.168.0.1, 192.168.0.0/24, 192.168.0.1-192.168.0.100

转换后端口 * 转换指定端口, 如: 80, 135:139

备注

插入到第 条之前