

ERG3 路由器对接 TP-Link IPSEC VPN（主模式）

1 配置需求或说明

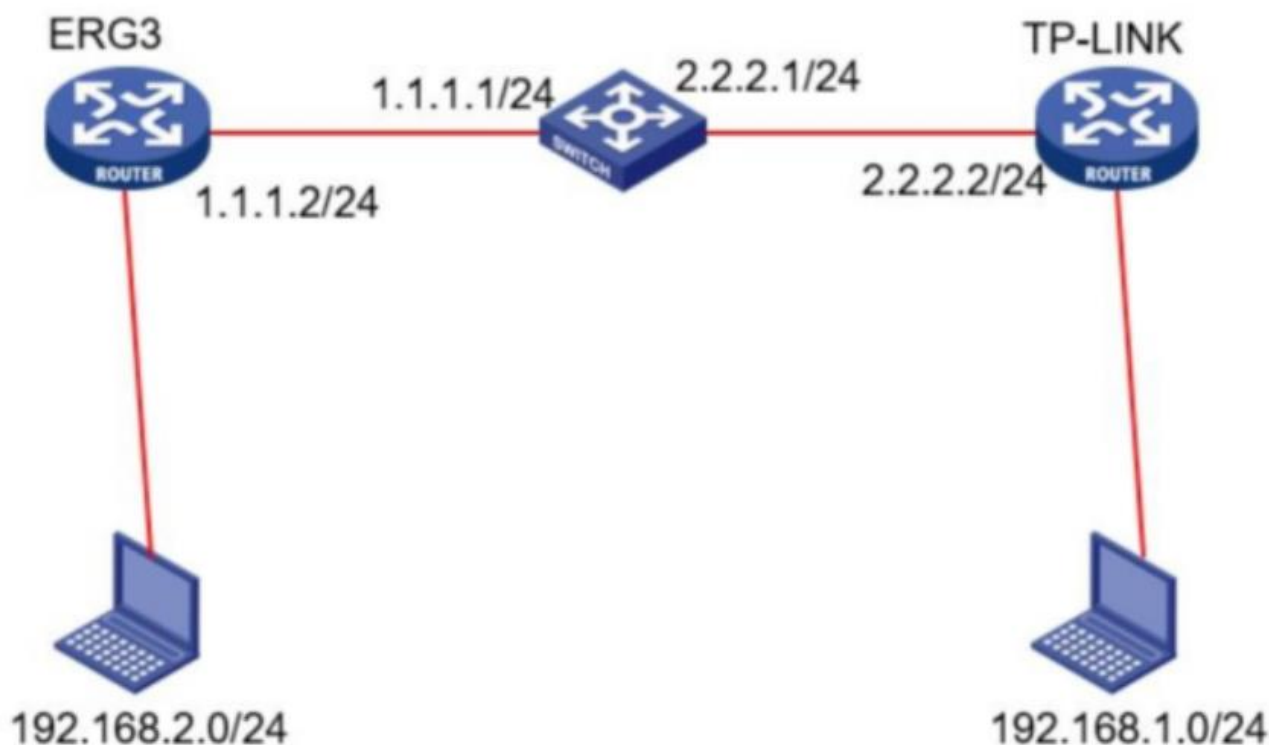
1.1 适用产品系列

本案例适用于 ERG3 系列路由器，如 ER5200G3、ER8300G3 等

1.2 配置需求及实现的效果

ERG3 和 TP 路由器分别作为企业网络的出口路由器，都有固定的公网地址，两个设备之间建立主模式的 IPSEC VPN，ERG3 内网网段为 192.168.2.0/24，TP 侧内网网段为 192.168.1.0/24

2 组网图



3 配置步骤

3.1 配置 ERG3

#正常配置内网口和外网口地址(此处省略，可以参考配置上网的案例)

#点击虚拟专网—ipsec—ipsec 策略—新增



#配置策略名称为test，接口选择外网口wan1，组网方式选择分支节点，对端地址写对端公网口地址2.2.2.2，预共享密钥，保护流分别写两端要互通的内网网段，配置完成后点击下一步

新增

1 基础信息 2 IKE配置 3 IPsec配置

* 策略名称 ① test

* 接口 WAN1

* 组网方式 ☒ 分支节点 ① ☐ 中心节点 ②

* 对端地址 ② 2.2.2.2

* 预共享密钥 ① ①

* 保护流措施 ②

受保护协议	本端网段/掩码	本端口	对端网段/掩码	对端口	操作
IP	192.168.2.0/255.255.255.0	0~65535	192.168.1.0/24	0~65535	+ -

取消 下一步

#配置 IKE，IKE 版本选择 V1，协商模式选择主模式，本端和对端身份类型都选择 IP 地址，两端的身份分别填写两端公网口的地址，算法组合选择自定义，配置加密算法为 3DES-CBC，认证算法为 MD5，PFS 选择 DH group1（两端的算法要保持一致），配置完成后点击下一步

新增

1 基础信息 2 IKE配置 3 IPsec配置

IKE 版本 ☒ V1 ☐ V2

协商模式 ☒ 主模式 (两端都有公网地址时推荐使用) ☐ 野蛮模式 (只有一端有公网地址时推荐使用)

本端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

本端身份 1 . 1 . 1 . 2

* 对端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

* 对端身份 2 . 2 . 2 . 2

对等体存活检测 (DPD) ☐

上一步 下一步

新增

×

本端身份 1 . 1 . 1 . 2

* 对端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

* 对端身份 2 . 2 . 2 . 2

对等体存活检测 (DPD) ☐

算法组合 自定义

* 认证算法 MD5

* 加密算法 3DES-CBC

* PFS DH group 1

SA生存时间 ① 86400 秒

上一步

下一步

#配置 ipsec,算法组合自定义,安全协议选择 ESP,认证算法为 MD5,加密算法为 3DES-CBC,封装模式选择隧道模式,触发模式选择自协商,配置完成后点击确认

新增

×

基础信息 ✓ IKE配置 ✓ IPSec配置 3

算法组合 自定义

* 安全协议 ☒ ESP ☐ AH

* ESP认证算法 MD5

* ESP加密算法 3DES-CBC

* 封装模式 ☐ 传输模式 ☒ 隧道模式

PFS None

SA生存时间 ① 3600 秒

触发模式 ☒ 自协商 ☐ 流量触发

上一步

确认

3.2 配置 TP-LINK

3.2.1 登录设备

电脑连接设备的 LAN 口, 自动获取地址, 默认登录地址为 192.168.1.1



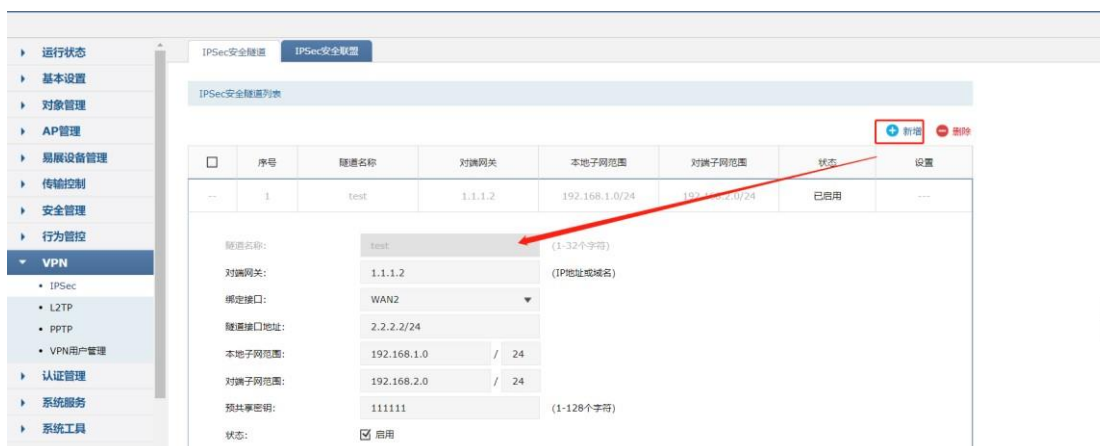
3.2.2 配置外网

【基本设置】--【WAN 配置】--【WAN2 配置】



3.2.3 配置 IPSEC VPN

【VPN】--【IPSEC】--【启用 VPN 功能】点击新增



点击高级设置

运行状态

基本设置

对象管理

AP管理

易展设备管理

传输控制

安全管理

行为管控

VPN

认证管理

系统服务

系统工具

快速配置

IPSec安全隧道

IPSec安全联盟

高级设置

阶段1设置

安全提议:

md5-3des-dh1

安全提议:

安全提议:

安全提议:

交换模式:

☒ 主模式 ☐ 野蛮模式

协商模式:

☒ 初始者模式 ☐ 响应者模式

本地ID类型:

☒ IP地址 ☐ NAME

本地ID:

(1-28个非空字符)

对端ID类型:

☒ IP地址 ☐ NAME

对端ID:

(1-28个非空字符)

生存时间:

28800

秒(60-604800)

DPD检测开启:

☒ 启用 ☐ 禁用

阶段2设置

封装模式:

☒ 隧道模式 ☐ 传输模式

安全提议:

esp-md5-3des

安全提议:

安全提议:

安全提议:

PFS:

none

生存时间:

28800

秒(120-604800)

确定

取消

3.3 结果验证

ping 可达

```
C:\Users\sys1392>ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=64

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
Control-C
^C
```

3.4 保存配置

默认都是自动保存