

ERG3 路由器对接华为路由器 IPSEC VPN（主模式）

1 配置需求或说明

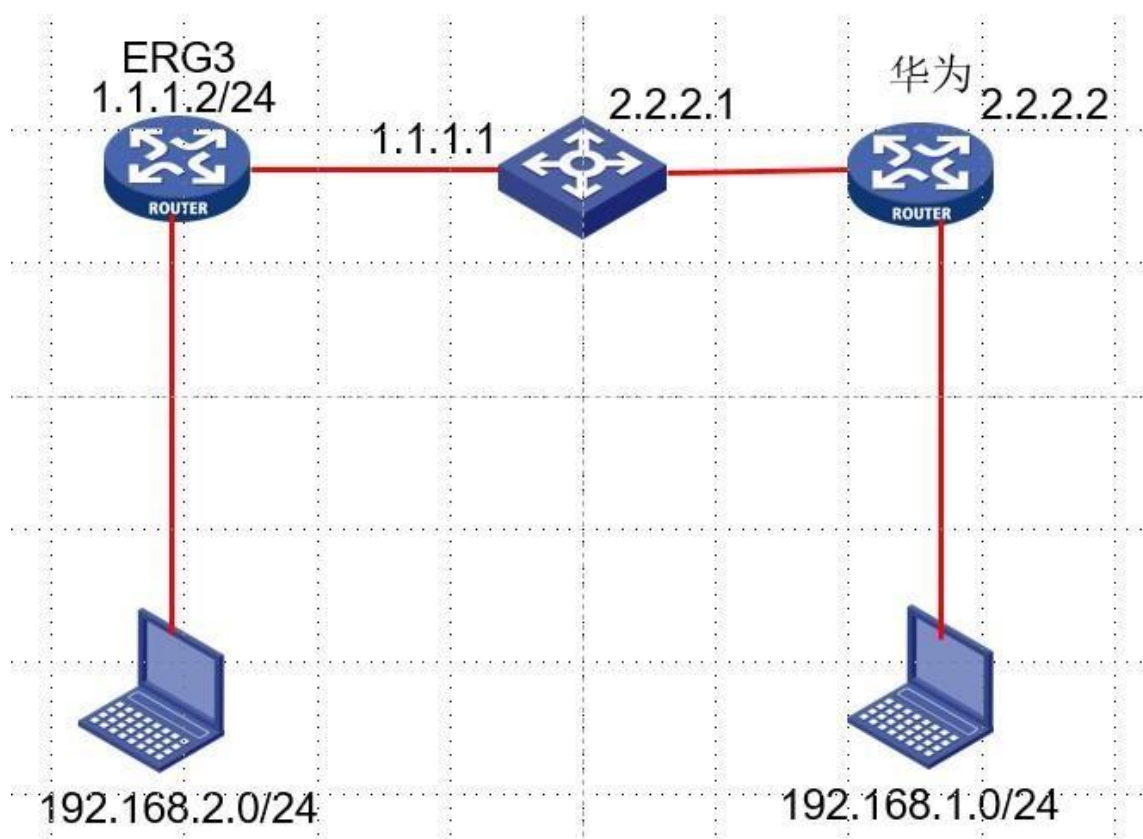
1.1 适用产品系列

本案例适用于 ERG3 系列路由器，

1.2 配置需求及实现的效果

ERG3 和 华为路由器分别作为企业网络的出口路由器，两端有固定的公网地址，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，华为侧内网网段为 192.168.1.0/24

2 组网图



3配置步骤

3.1 配置 ERG3

3.1.1 配置外网

#参考之前配置上网的案例进行配置，此处省略

3.1.2 配置 IPSEC VPN

#点击虚拟专网—ipsec—ipsec 策略—新增



#策略名称自定义，接口选择对接 VPN 的外网口，组网方式选择分支节点，对端地址填写对端公网口地址 2.2.2.2，预共享密钥两端配置一致，保护流填写两端需要互通的内网网段，配置完成后点击下一步

×

新增

1

2

3

基础信息

IKE配置

IPSec配置

* 策略名称 ?

test

* 接口

WAN1

* 组网方式

分支节点 ?

中心节点 ?

* 对端地址 ?

2.2.2.2

* 预共享密钥 ?

.....

* 保护流措施 ?

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

取消

下一步

#配置 ike 配置，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，两端的身份写两端公网口的地址，认证算法 MD5，加密算法 3DES-CBC，PFS 为 dh1（两端的加密认证算法需要配置一致），配置完成后点击下一步

新增

×

✓

2

3

基础信息IKE配置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 ⓘ

86400

秒

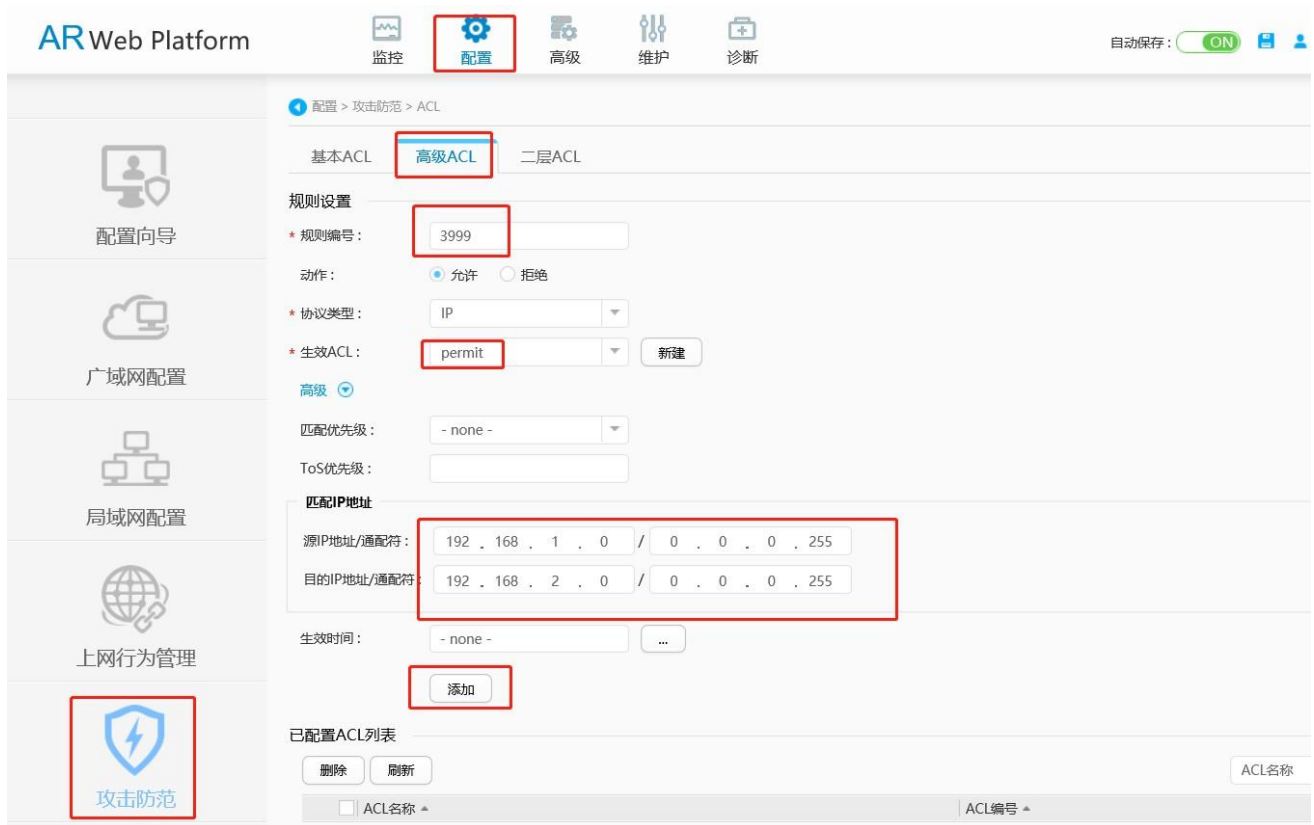
上一步

下一步

#配置 ipsec 参数，安全协议为 ESP，认证算法 MD3，加密算法 3DEC-CBC，封装模式选择隧道模式，配置完成后点击确认

➤

【配置】--【广域网配置】--固定外网口地址



3.2.3 配置 IPSEC VPN

【配置】--【配置向导】--【IPSEC 配置向导】



继续往下操作

1.选择接入类型

2.配置加密与认证

3.定义受保护的数据流

☒ 站点到站点☐ 中心站点☐ 分支站点

该场景用来配置网关到网关的连接中,可配置任何一端的网关。



配置网络

* 选择以太接口: GigabitEthernet0/0/4

* 对端地址: 1.1.1.2

Ping测试

结果显示:

下一步

取消

IPSec配置向导

1.选择接入类型

2.配置加密与认证

3.定义受保护的数据流

配置隧道加密与认证参数,包括IKE和IPSec。

* 预共享密钥: *****

IKE参数配置

协商模式: 主模式

认证算法: MD5 (该算法的安全级别低)

加密算法: 3DES (该算法的安全级别低)

DH组编号: Group1

IPSec参数配置

安全协议: ESP

ESP认证算法: MD5 (该算法的安全级别低)

ESP加密算法: 3DES (该算法的安全级别低)

封装模式: ☒ 隧道模式 ☐ 传输模式

上一步

下一步

取消

IPSec配置向导

1.选择接入类型

2.配置加密与认证

3.定义受保护的数据流

输入数据流源IP和目的IP,如果不输入,点击"添加"默认保护所有数据流。

源IP/通配符: . . . / . . .

目的IP/通配符: . . . / . . . +

已添加数据流

删除

☐ 源IP/通配符

☐ 192.168.1.0/0.0.0.255

目的IP/通配符

192.168.2.0/0.0.0.255

上一步

完成

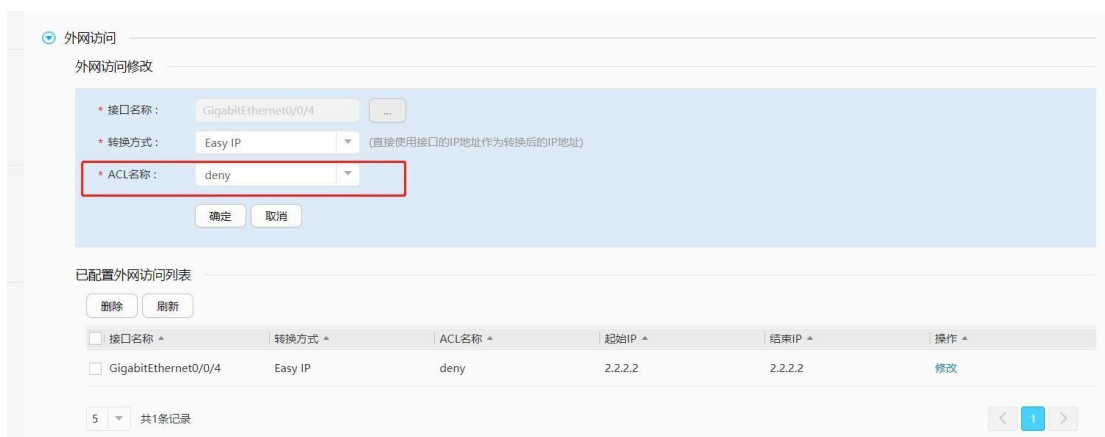
取消

【配置】--【攻击防范】--【ACL】

↓ deny 3999

规则...	动作	源IP地址/通配符	目的IP地址/通配符	协议类型	源端...	目的...	生效时间	操作
3999	拒绝	192.168.1.0/0.0.0.255	192.168.2.0/0.0.0.255	IP	--	--		修改 删除 详情

外网口拒绝 ACL



3.3 保存配置

默认都是自动保存