

UR 路由器对接锐捷路由器 IPSEC VPN（野蛮模式）

1 配置需求或说明

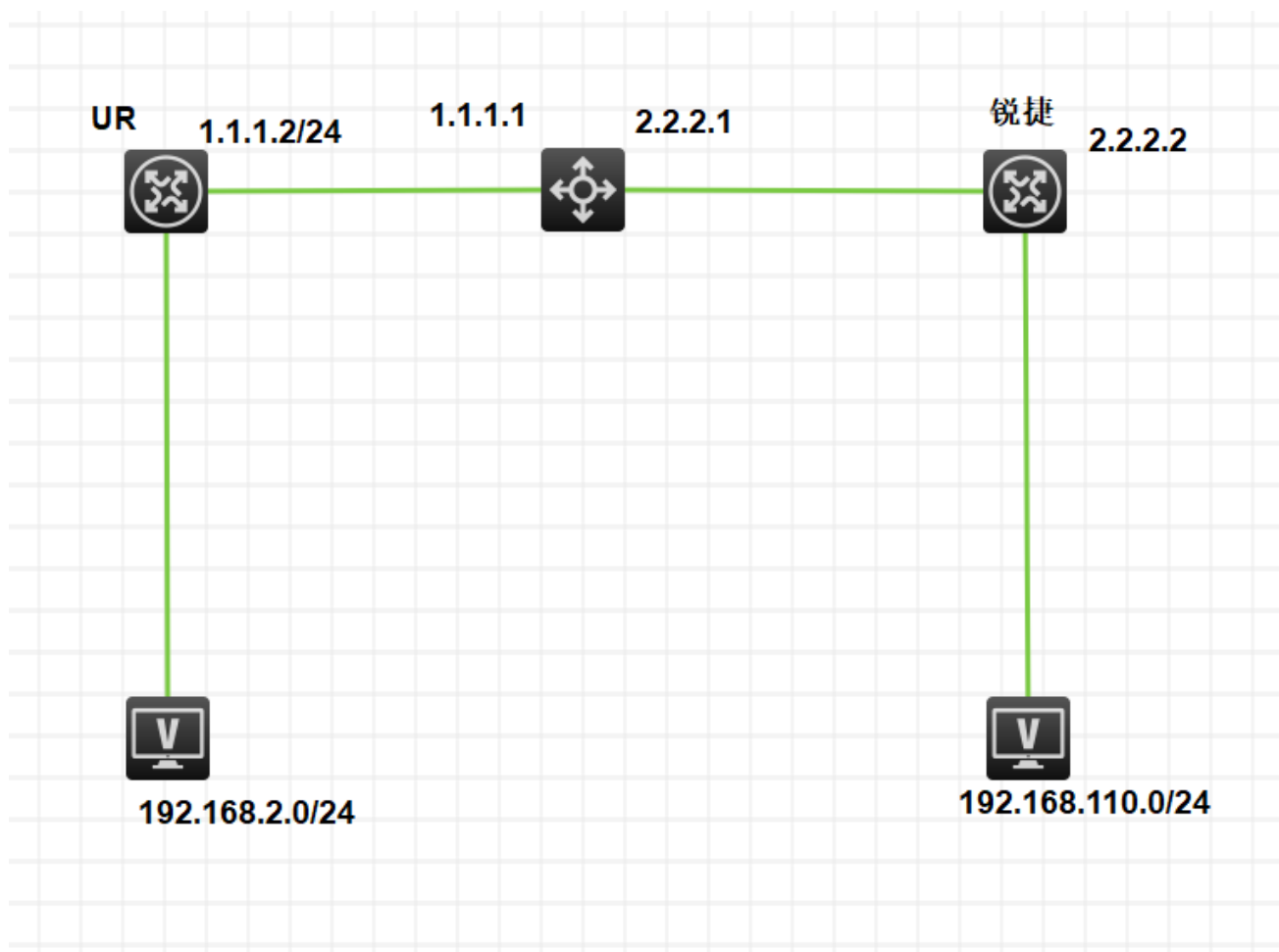
1.1 适用产品系列

本案例适用于 UR 系列路由器，

1.2 配置需求及实现的效果

UR 和锐捷路由器分别作为企业网路的出口路由器，UR 有固定的公网地址，锐捷设备没有固定公网地址，两个设备之间建立主模式的 IPSEC VPN，UR 内网网段为 192.168.2.0/24，锐捷侧内网网段为 192.168.110.0/24

2 组网图



3 配置步骤

3.1 配置 UR

3.1.1 配置外网

#参考之前配置上网的案例，此处省略

3.1.2 配置 IPSEC VPN

#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，组网方式选择中心节点，预共享密钥，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 ①

test

* 接口

WAN1

* 组网方式

分支节点 ①

中心节点 ②

* 预共享密钥 ①

取消

下一步

#配置 IKE，IKE 版本选择 V1，协商模式选择野蛮模式，两端身份类型都选择 IP 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

对等体存活检测 (DPD)

☐

算法组合

自定义

* 认证算法

MD5

上一步

下一步

新增

1

基础信息

2

IKE配置

3

IPSec配置

协商模式

☒ 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,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

3IPSec配置

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

3600

秒

触发模式

自协商

流量触发

上一步

确认

3.2 配置锐捷设备

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 192.168.110.1

3.2.2 配置外网

【路由管理】--【基本管理】--【WAN 设置】

整网概览

在线用户

路由管理

无线管理

交换管理

整网管理

名称: Ruijie
MAC地址: 9C:2B:

设备概览 基本管理 安全管理

WAN设置
LAN设置
IPSec安全策略
IPv6设置
端口VLAN

单/双线路 三线路 四线路

WAN

WAN1

运营商/负载设置

* 联网类型 静态IP

* IP地址 2.2.2.2

* 子网掩码 255.255.255.0

* 网关地址 2.2.2.1

* DNS服务器 114.114.114.114

高级模式

保存

3.2.3 配置 IPSEC VPN

【路由管理】--【VPN 管理】--【IPSEC 设置】

路由管理

无线管理

交换管理

整网管理

设备概览 基本管理 安全管理 行为管理 VPN管理 高级管理

WAN设置
上网配置页面

单/双线路 三线路 四线路

IPSec设置
L2TP
PPTP
用户管理

点击添加

策略类型

☒ 客户端

☐ 服务端

* 策略名称

test

* 对端网关

1.1.1.2

+

绑定接口

WAN

?

* 本地子网范围

192.168.110.0/24

* 对端子网范围

192.168.2.0/24

+

* 预共享密钥

111111

状态

☒

阶段一设置 (IKE策略)

IKE策略 1

md5-3des-dh1

▼

IKE策略 2

md5-des-dh2

▼

IKE策略 3

sha1-3des-dh2

▼

IKE策略 4

md5-des-dh1

▼

IKE策略 5

md5-3des-dh2

▼

协商模式

☐ 主模式

☒ 野蛮模式

本地ID类型

☒ IP地址

☐ NAME

对端ID类型

☒ IP地址

☐ NAME

* 生存时间

86400

DPD检测开启

☐ 启用

☒ 未启用

阶段二设置 (建立连接策略)

转换集1 esp-md5-3des

转换集2 esp-md5-aes256

完美向前加密 none

* 生存时间 3600

取消 确定

3.3 结果验证

ping 触发后，查看隧道信息

```
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=2ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=2ms TTL=63

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 2ms, 平均 = 2ms
Control-C
^C
```

锐捷侧:

IPSec连接状态 刷新								
名称	SPI	方向	隧道两端	数据流	状态	安全协议	算法	
test	3274170826	in	2.2.2.2<--1.1.1.2	192.168.110.0/24 <-- 192.168.2.0/24	正常	ESP	AH验证算法: -- ESP验证算法: MD5 ESP加密算法: 3DES	
test	3384690989	out	2.2.2.2-->1.1.1.2	192.168.110.0/24 --> 192.168.2.0/24	正常	ESP	AH验证算法: -- ESP验证算法: MD5 ESP加密算法: 3DES	

UR 侧:

☐	策略名称 ▲	状态	接口	本端地址	对端地址	安全提议	操作
☐	test	up	WAN1	1.1.1.2	2.2.2.2	3DES_CBC/HMAC_MD5_96/...	🔗➡

3.4 保存配置

默认都是自动保存