

UR 系列路由器 IPSEC VPN 配置（主模式）

1 配置需求或说明

1.1 适用产品系列

本案例适用于小贝优选 UR 系列路由器：UR7504、UR7808、UR7103 等。

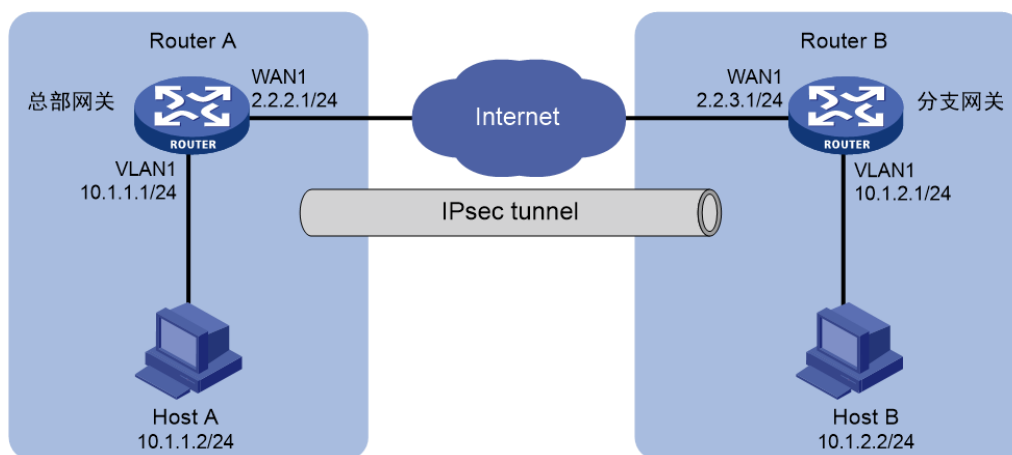
1.2 配置需求及实现的效果

Router A 为企业总部网关，Router B 为企业分支网关，Router A 和 Router B 的外网接口模式均以固定地址方式连接 Internet。分支与总部通过公网建立通信。

出于安全因素，需要对企业分支与总部之间相互访问的数据流进行安全保护，因此需要在 Router A 和 Router B 之间建立一条 IPsec 隧道。具体要求如下：

- 两端通过预共享密钥（123456TESTplat&!）进行认证。
- IKE 协商采用的加密算法为 3DES-CBC，认证算法为 MD5。
- IPsec 隧道的封装模式为隧道模式，安全协议为 ESP。

2、组网图



3 配置步骤

3.1 配置 Router A

#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 map1，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 2.2.3.1，预共享密钥 123456TESTplat&!，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 ② map1

* 接口 WAN1

* 组网方式 ☒ 分支节点 ② ☐ 中心节点 ②

* 对端地址 ② 2.2.3.1

* 预共享密钥 ② 123456TESTplat&!

* 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	10.1.1.0/255.255.255.0	0~65535	10.1.2.0/255.255.255.0	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 group2（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 2 . 2 . 2 . 1

* 对端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

* 对端身份 2 . 2 . 3 . 1

对等体存活检测 (DPD) ☐

上一步 下一步

新增

本端身份 2 . 2 . 2 . 1

* 对端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

* 对端身份 2 . 2 . 3 . 1

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 2

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 DES-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

算法组合 自定义

* 安全协议 ☒ ESP ☐ AH

* ESP认证算法 MD5

* ESP加密算法 DES-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 Router B

#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

虚拟专网 / IPsec / IPsec策略

IPsec策略 监控信息

刷新 新增 批量删除

请输入

策略名称	组网方式	接口	本端地址	对端地址	管理状态
暂无数据					

已选择 0 项 | 共有 0 条

1 10条/页

#配置策略名称为 map1，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 2.2.2.1，预共享密钥 123456TESTplat&!，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

2

3

基础信息IKE配置IPSec配置

* 策略名称 ②

map1

* 接口

WAN1

* 组网方式

☒ 分支节点 ②

☐ 中心节点 ②

* 对端地址 ②

2.2.2.1

* 预共享密钥 ②

🔒

.....

🔓

* 保护措施 ②

受保护协议	本端网段/掩码	本端端口	对端网段/掩码	对端口	操作
IP	10.1.2.0/255.255.255.0	0-65535	10.1.1.0/255.255.255.0	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 group2（两端的算法要保持一致），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

IKE 版本

☒ V1

☐ V2

协商模式

☒ 主模式

☐ 野蛮模式

两端都有公网地址时推荐使用)

(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

2 . 2 . 3 . 1

* 对端身份类型

☒ IP地址

☐ FQDN

☐ User-FQDN

* 对端身份

2 . 2 . 2 . 1

对等体存活检测 (DPD)

☐

上一步

下一步

新增

本端身份 2 . 2 . 3 . 1

* 对端身份类型 ☒ IP地址 ☐ FQDN ☐ User-FQDN

* 对端身份 2 . 2 . 2 . 1

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 2

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 DES-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 DES-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

3.3 保存配置

设备默认会保存配置。

4 验证配置

(1) 用 Host A 主机 ping Host B 主机 IP 地址, 可以 ping 通。

```
C:\Users\abc>ping 10.1.2.2
```

```
Ping 10.1.2.2 (10.1.2.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
```

```
56 bytes from 10.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms
```

```
--- Ping statistics for 10.1.2.2 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

```
C:\Users\abc>
```

- (2) 完成上述配置后，在设备 Web 管理界面选择“虚拟专网(VPN) > IPsec VPN”，单击“监控信息”页签，进入监控信息页面，可以看到建立成功的 IPsec 隧道信息，状态列显示为 UP，说明配置验证成功。