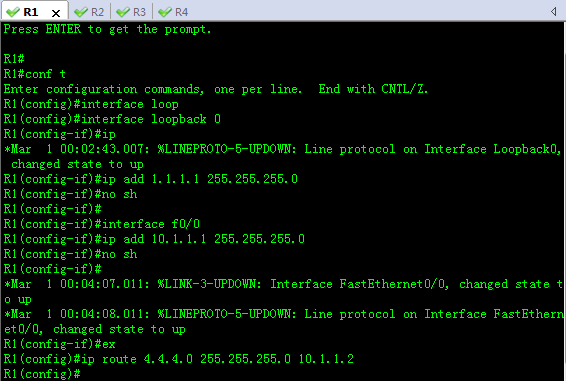


实验十二：VPN

需求：

基本网络配置：



R1:

R1(config)#interface loopback 0

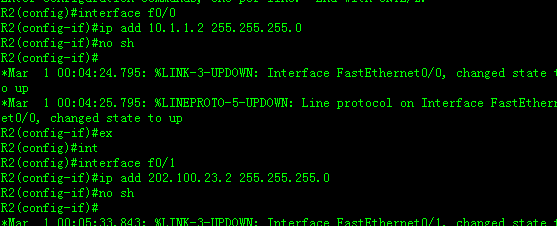
R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#no sh

R1(config)#interface f0/0

R1(config-if)#ip address 10.1.1.1 255.255.255.0

R1(config-if)#no sh



R2:

R2(config)#interface f0/0

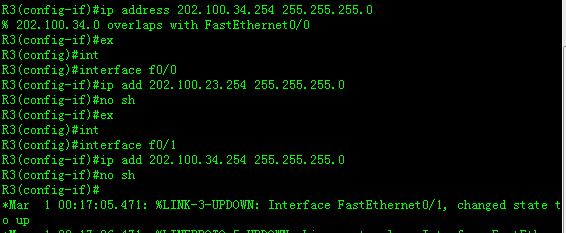
R2(config-if)#ip add 10.1.1.2 255.255.255.0

R2(config-if)#no shutdown

R2(config)#interface f0/1

R2(config-if)#ip add 202.100.23.2 255.255.255.0

R2(config-if)#no shutdown



R3:

R3(config)#interface f0/0

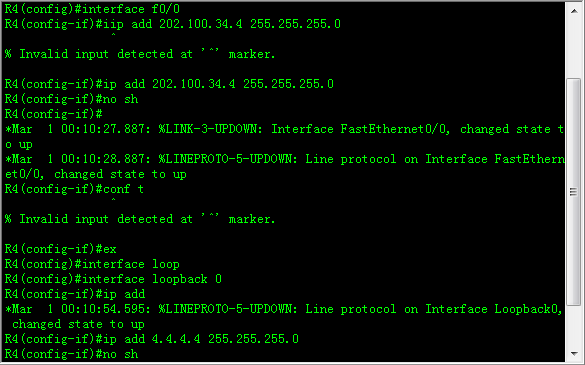
R3(config-if)#ip address 202.100.23.254 255.255.255.0

R3(config-if)#no shutdown

R3(config)#interface f0/1

R3(config-if)#ip address 202.100.34.254 255.255.255.0

R3(config-if)#no shutdown



R4:

R4(config)#interface f0/0

R4(config-if)#ip address 202.100.34.4 255.255.255.0

R4(config-if)#no shutdown

R4(config)#interface loopback 0

R4(config-if)#ip address 4.4.4.4 255.255.255.0

R4(config-if)#no shutdown

路由分析：

三大类路由解决：

本端通信点，远端加密点，远端通信点

R1:

要解决去往远端通信点的路由（4.4.4.0/24）

R2:

要解决本地通信点路由（1.1.1.0/24）

要解决远端加密点路由（202.100.34.0/24）

要解决远端通信点路由（4.4.4.0/24）

R3:

要解决两端加密点路由（202.100.12.0/24）(202.100.34.0/24)

R4：

要解决本地通信点路由（4.4.4.0/24）

要解决远端加密点路由（202.100.12.0/24）

要解决远端通信点路由（1.1.1.0/24）

配置如下：

R1:

要解决去往远端通信点的路由（4.4.4.0/24）

R1(config)#ip route 4.4.4.0 255.255.255.0 10.1.1.2



R2：

要解决本地通信点路由（1.1.1.0/24）

R2(config)#ip route 1.1.1.0 255.255.255.0 10.1.1.1

要解决远端加密点路由（202.100.34.0/24）

R2(config)#ip route 202.100.34.0 255.255.255.0 202.100.23.254

要解决远端通信点路由（4.4.4.0/24）

R2(config)#ip route 4.4.4.0 255.255.255.0 202.100.23.254

R3:

要解决两端加密点路由（202.100.12.0/24）(202.100.34.0/24)

注意：这里由于是实验环境，因此有直连路由。一般真实环境由BGP代替



R4：

要解决本地通信点路由（4.4.4.0/24）由于是环回口，有直连路由，一般真实环境由IGP代替

要解决远端加密点路由（202.100.12.0/24）

R4(config)#ip route 202.100.23.0 255.255.255.0 202.100.34.254

要解决远端通信点路由（1.1.1.0/24）

R4(config)#ip route 1.1.1.0 255.255.255.0 202.100.34.254

IPsec VPN经典配置：

R2:

第一阶段：

R2(config)#crypto isakmp enable //默认已开启。

R2(config)#crypto isakmp policy 10 //创建IKE第一阶段策略。策略编号为10

R2(config-isakmp)#encryption 3des //IKE数据包加密算法使用3DES。默认使用DES

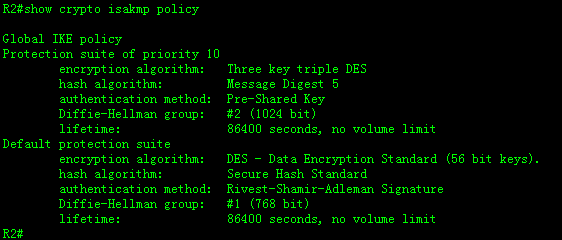
R2(config-isakmp)#hash md5 //IKE数据包完整性校验的散列算法使用md5。默认使用SHA-1

R2(config-isakmp)#authentication pre-share //IKE第一阶段5-6个包，认证方式使用预共享密钥。默认使用数字签名。

R2(config-isakmp)#group 2 //IKE第一阶段3-4个包，DH交换使用group2。默认使用group1

R2(config)#crypto isakmp key 0 cisco address 202.100.34.4 //IKE第一阶段5-6个包，与共享密钥为cisco

R2#show crypto isakmp policy //查询第一阶段的配置



第二阶段：

感兴趣流：

R2(config)#ip access-list extended lsj

R2(config-ext-nacl)#permit ip 1.1.1.0 0.0.0.255 4.4.4.0 0.0.0.255 //满足这个抓取的数据会被加密，也就是通信点之间的流量。

变换集（转换集）：

R2(config)#crypto ipsec transform-set myset esp-3des esp-sha-hmac //加密数据的具体策略名字为myset，使用ESP封装，加密使用3DES，完整性校验使用SHA-HMAC

R2(cfg-crypto-trans)#mode tunnel //模式使用隧道模式。典型的通信点不等于加密点。默认使用隧道模式。

配置Crypto map(加密图):

R2(config)#crypto map ccie 10 ipsec-isakmp //配置名字为ccie,ID为10的Map，一个ID标示一个VPN。一个MAP可以有多个ID，一个接口只能运用一个MAP。

R2(config-crypto-map)#match address lsj //匹配感兴趣流

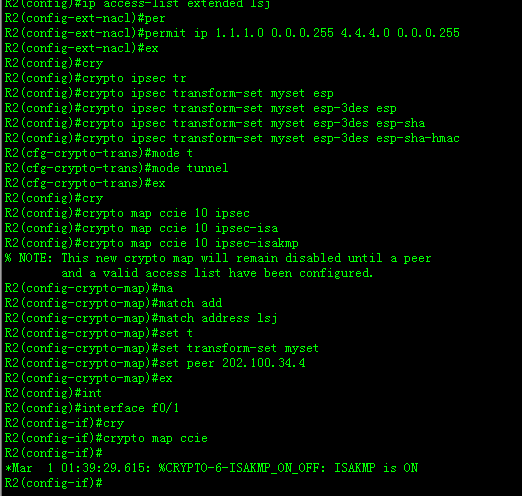
R2(config-crypto-map)#set transform-set myset //使用什么策略来加密感兴趣流

R2(config-crypto-map)#set peer 202.100.34.4 //和谁建立VPN。对端公网IP

调用Crypto map 到接口：

R2(config)#interface f0/1

R2(config-if)#crypto map ccie //调用加密图



R4:

第一阶段：

R4(config)#crypto isakmp enable //默认已开启。

R4(config)#crypto isakmp policy 10 //创建IKE第一阶段策略。策略编号为10

R4(config-isakmp)#encryption 3des //IKE数据包加密算法使用3DES。默认使用DES

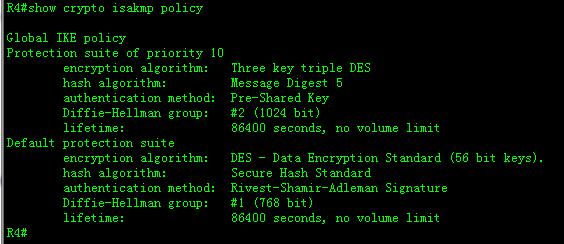
R4(config-isakmp)#hash md5 //IKE数据包完整性校验的散列算法使用md5。默认使用SHA-1

R4config-isakmp)#authentication pre-share //IKE第一阶段5-6个包，认证方式使用预共享密钥。默认使用数字签名。

R4(config-isakmp)#group 2 //IKE第一阶段3-4个包，DH交换使用group2。默认使用group1

R4(config)#crypto isakmp key 0 cisco address 202.100.23.2 //IKE第一阶段5-6个包，与共享密钥为cisco

R4#show crypto isakmp policy //查询第一阶段的配置



第二阶段：

感兴趣流：

R4(config)#ip access-list extended lsj

R4(config-ext-nacl)#permit ip 4.4.4.0 0.0.0.255 1.1.1.0 0.0.0.255 //满足这个抓取的数据会被加密，也就是通信点之间的流量。

变换集（转换集）：

R4(config)#crypto ipsec transform-set myset esp-3des esp-sha-hmac //加密数据的具体策略名字为myset，使用ESP封装，加密使用3DES，完整性校验使用SHA-HMAC

R4(cfg-crypto-trans)#mode tunnel //模式使用隧道模式。典型的通信点不等于加密点。默认使用隧道模式。

配置Crypto map(加密图):

R4(config)#crypto map ccie 10 ipsec-isakmp //配置名字为ccie,ID为10的Map，一个ID标示一个VPN。一个MAP可以有多个ID，一个接口只能运用一个MAP。

R4(config-crypto-map)#match address lsj //匹配感兴趣流

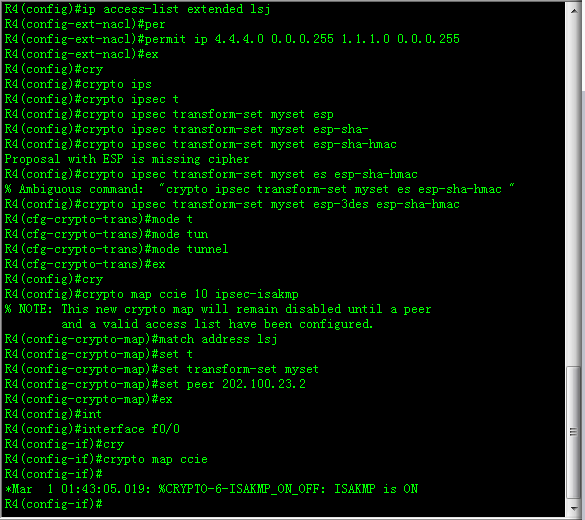
R4(config-crypto-map)#set transform-set myset //使用什么策略来加密感兴趣流

R4(config-crypto-map)#set peer 202.100.23.2 //和谁建立VPN。对端公网IP

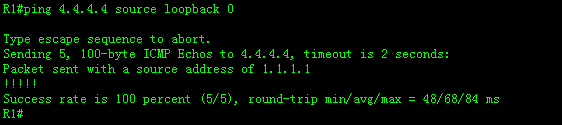
调用Crypto map 到接口：

R4(config)#interface f0/0

R4(config-if)#crypto map ccie //调用加密图



测试VPN加密情况：



R2#show crypto ipsec sa



