**江苏科技大学**

**课程设计报告**

课 程： 计算机网络与安全课程设计

课 题： 动态crypto map实验

学 院： 计算机学院

小组成员： 182210710119 陈四贵

182210710118 陈 鳌

182210710108 李川越

182210710137 张震宇

班 级： 1822107101

指导老师： 张笑非

目 录

[一、 实验目的 1](#_Toc59877382)

[二、 实验原理暨实验步骤 1](#_Toc59877383)

[三、 实验内容暨实验结果 1](#_Toc59877384)

[四、 实验总结与思考 5](#_Toc59877385)

# 实验目的

1. 了解crypto map实验拓扑情况，并能作出基本配置；

2. 通过crypto map实验进一步理解影响IPsec vpn的网络问题。

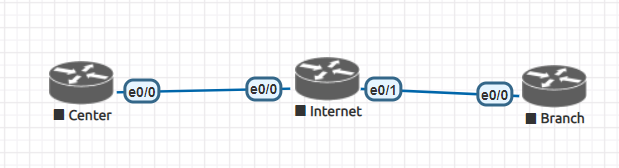
3. 熟悉eve的使用。

# 实验原理暨实验步骤

配置路由器的IP地址和路由，执行基本网络配置，再配置动态crypto map IPSec VPN。

# 实验内容暨实验结果

**Step 1**，创建crypto拓扑结构，即中心站点的VPN网关路由器（Center）、分支站点的VPN网关服务器（Branch）以及位于此间的Internet。



**Step 2**，配置路由器的IP地址与路由，即执行基本网络配置。

2.1 Center上的基本网络配置

1. enable
2. config t
3. hostname Center
4. interface Loopback0
5. ip address 1.1.1.1 255.255.255.0
6. interface e0/0
7. ip address 202.100.1.1 255.255.255.0
8. no shutdown
9. ip route 0.0.0.0 0.0.0.0 202.100.1.10
10. end

2.2 Internet上的基本网络配置

1. enable
2. config t
3. hostname Internet
4. ip dhcp pool Branch
5. network   61.128.1.0   255.255.255.0
6. **default**-router   61.128.1.10
7. interface e0/0
8. ip address   202.100.1.10   255.255.255.0
9. no shutdown
10. interface e0/1
11. ip address   61.128.1.10   255.255.255.0
12. no shutdown
13. end

2.3 Branch上的基本网络配置

1. enable
2. config t
3. hostname Branch
4. interface Loopback0
5. ip address   2.2.2.2   255.255.255.0
6. interface e0/0
7. ip address dhcp
8. no shutdown
9. end

**Step 3**，配置完成后，查看Branch获取IP地址后Console口显示的信息，Branch接口的IP地址及通过DHCP获取的默认路由，并测试网络连通性。

涉及命令：

1. show ip interface brief
2. show ip route
3. ping 202.100.1.1

**Step 4**，配置Branch经典站点到站点IPSec VPN

1. crypto isakmp policy 10
2. authentication pre-share
3. crypto isakmp key 0 cisco address 202.100.1.1
4. ip access-list ex vpn
5. permit  ip  2.2.2.0  0.0.0.255  1.1.1.0  0.0.0.255
6. crypto ipsec transform-set cisco esp-des esp-md5-hmac
7. crypto map cisco 10 ipsec-isakmp
8. match address vpn
9. set transform-set  cisco
10. set peer 202.100.1.1
12. interface e0/0
13. crypto map cisco

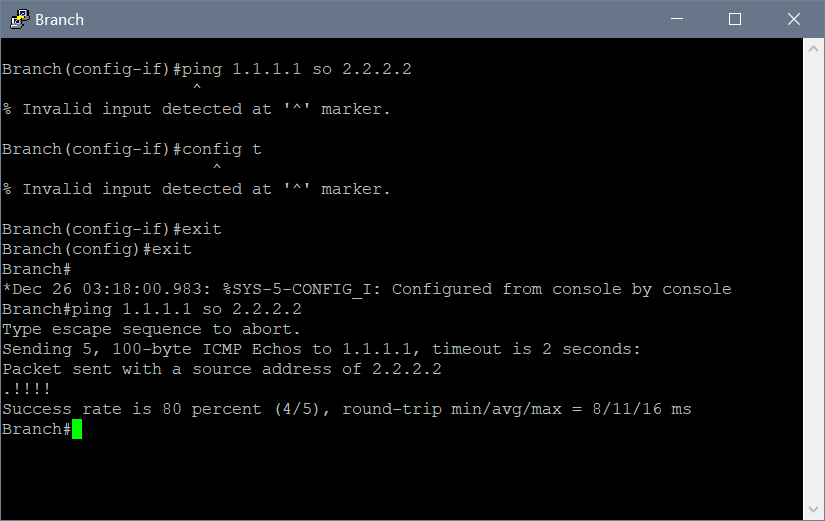
**Step 5**，配置Center动态crypto map IPSec VPN

1. crypto isakmp policy 10
2. authentication pre-share
4. crypto isakmp key 0 cisco address 0.0.0.0 0.0.0.0
5. crypto ipsec transform-set cisco esp-des esp-md5-hmac
6. crypto dynamic-map dymap 10
7. set transform-set cisco
8. crypto map cisco 10000 ipsec-isakmp dynamic dymap
9. interface e0/0
10. crypto map cisco

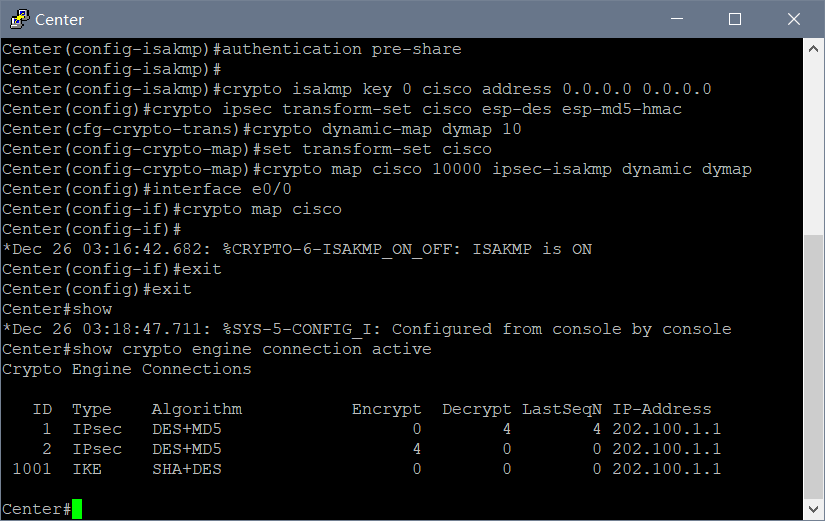
**Step 6**, 测试IPSec VPN

涉及命令：

1. ping 1.1.1.1 so 2.2.2.2
2. ping 2.2.2.2 so 1.1.1.1
3. show crypto engine connections active

6.1 在Branch上执行ping操作，向Center主动发起IPSec VPN

6.2 在Center上执行show crypto engine connection active命令，查看加解密状态。



# 实验总结与思考

动态crypto map作为IPSec VPN的配置方式之一，存在一些缺点：

1、中心站点不能主动发起IPSec VPN，因为中心站点并不知道分支站点的IP地址和感兴趣流；

2、这种配置方法没有使用虚拟隧道接口，不能在中心和分支站点间贯通动态路由协议，更不能使用ACL、QoS和NAT等技术对明文流量进行有效地控制。