**《网络互连实训》参考文档**

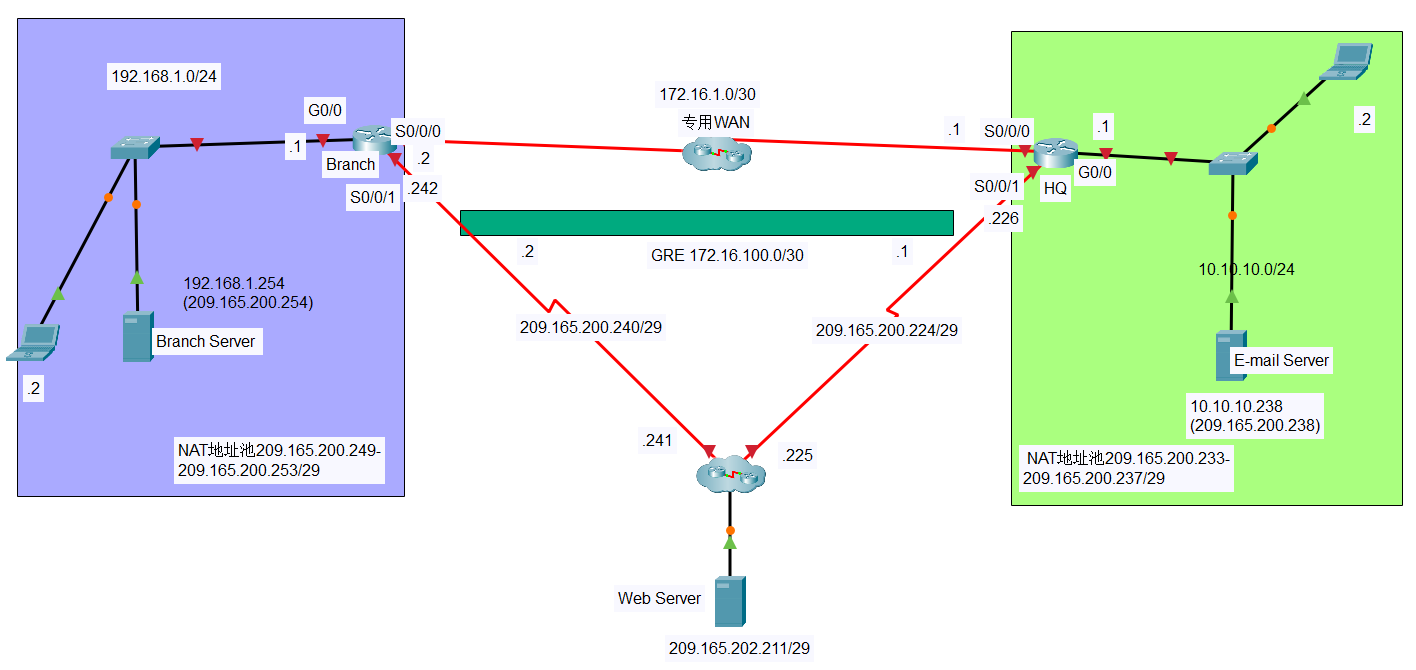
**一、任务与目的**

通过实验，学生可扩大、巩固已学专业课程的知识，使学生分析问题、解决实际工程问题的能力得到培养和训练，培养学生建立正确的思维方法、严谨的科学作风、提高分析解决问题的能力和抽象思维能力。使学生掌握主流路由器的以及各种协议的配置技术，包括ospf基础知识及其配置、NAT地址转换配置、Tunnel基本概念及配置、ipsec、GRE Tunnel、VPN基本概念及配置等技术。学生根据题目的要求，利用所学的知识在理解的基础上，利用现有设备构建网络，对相关设备进行配置及系统调试，完成任务。

**二、基本内容与要求**

1、实验内容

* 参见图1，企业两个分支机构，两个分支机构平时通过Internet通信，Internet故障时才通过备用的专用WAN线路通信。配置完成后，一旦Internet出故障，企业两个分支机构的通信自动切换到备用的专用WAN线路。
* VPN技术的主要目标是降低企业的通信成本，特别是替代企业已有的专线，并且提高企业网络的可管理性。关闭WAN专线，在Internet上构建GRE VPN负责企业两个分支机构的通信。
* 以上两个任务各自完成时，都不能把企业的私有网络暴露在公网上，企业内部的计算机都能访问公网。



**图1 网络拓扑**

2、配置要求

* BRANCH用户与HQ用户通过Internet构建的IPSec VPN通信，专用WAN链路为备份电路。当VPN线路故障时，专用WAN链路自动上线（提示：使用浮动静态路由,OSPF的管理距离+1）。

BRANCH(config)#intf0/0

BRANCH(config-if)#ip add xxx

BRANCH(config-if)#no sh

……

BRANCH(config)#int tunnel 0

BRANCH(config-if)#tunnel source s0/0/1

BRANCH(config-if)#tunnel destination 209.165.200.226

BRANCH(config-if)#ip add 172.16.100.2

BRANCH(config-if)#tunnel gre ip

HQ同理

* BRANCH路由器和HQ路由器通过OSPF协议（进程号1，area 0）把直连的三个私有网络号联成一个通信区域，以便BRANCH用户与HQ用户通信。

BRANCH(config)#router ospf 1

BRANCH(config-router)#net 172.16.100.0 0.0.0.3 area 0

BRANCH(config-router)#net 192.168.1.0 0.0.0.255 area 0

BRANCH(config-router)#exit

HQ(config)# router ospf 1

HQ(config-router)#net 172.16.100.0 0.0.0.3 area 0

HQ(config-router)#net 10.10.10.0 0.0.0.255 area 0

BRANCH(config-router)#exit

* HQ LAN位于网络10.10.10.0/24中。它还有一台供分支机构用户访问的E-mail服务器。外网用户也可通过Internet访问E-mail服务器；访问时将目标地址指定为公有地址209.165.200.238，将使用静态NAT将该地址转换为E-mail服务器的内部地址。

HQ(config)#ip nat pool HQ-pool 209.165.200.233 209.165.200.237 netmask 255.255.255.248

HQ(config)#ip access-list extended HQ-NAT-ACL

HQ(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255

HQ(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any

HQ(config-ext-nacl)#exit

HQ(config)#ip access-list extended 101

HQ(config-ext-nacl)#permit gre host 209.165.200.226 host 209.165.200.242

HQ(config-ext-nacl)#exit

HQ(config)#ip nat inside source static 10.10.10.238 209.165.200.238

HQ(config)#ip nat inside source list HQ-NAT-ACL pool HQ-pool overload

HQ(config)#int f0/0

HQ(config-if)#ip nat inside

HQ(config-if)#int s0/0/1

HQ(config-if)#ip nat outside

* BRANCH LAN位于网络192.168.1.0/24中。其中也有一台服务器，HQ LAN用户将使用IP地址192.168.1.254来访问它，外网用户也可通过Internet访问。

Branch(config)#ip access-list extened BRANCH-NAT-ACL

Branch(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255

Branch(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any

Branch(config-ext-nacl)#exit

Branch(config)#ip access-list extened 101

Branch(config-ext-nacl)#permit gre host 209.165.200.242 host 209.165.200.226

Branch(config-ext-nacl)#exit

Branch(config)#ip nat inside source static 192.168.1.254 209.165.200.254

Branch(config)#ip nat pool BRANCH-pool 209.165.200.249 209.165.200.253 netmask 255.255.255.248

Branch(config)#ip nat inside source list BRANCH-NAT-CAL pool BRANCH-pool overload

* BRANCH用户与HQ用户NAT 地址转换后,通过默认路由来访问Internet。

Branch(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

Branch(config)#ip route 10.10.10.0 255.255.255.0 172.16.1.1 111

HQ(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1

HQ(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2 111

**三、验收**

若选用真机完成配置，通过指导教师当场验证后，加分。全体同学参加pka测试代替传统的实验报告。

2.IPSec站点到站点VPN的配置

配置验证IPSec VPN，必须理解一些概念。配置IPSec VPN的步骤如下。

(1)配置初始密钥(ISAKMP) 。

(2)配置IPSec。

(3) 配置加密ACL。

(4) 配置VPN隧道。

(5)应用加密映射表。

**BRANCH路由器ipsec VPN配置举例：**

crypto isakmp policy 100（进入IKE策略编辑模式，100代表优先级）

encryption aes（封装aes）

authentication pre-share（使用预共享认证模式）

group 5(使用Diffie-Hellma (使用Diffie-Hellman 组5进行密钥交换)

crypto isakmp key cisco address 209.165.200.226（定义预--共享密钥）

crypto ipsec transform-set BRANCH-Set esp-aes esp-sha-hmac(配置IPsec的变换集，对数据交换进行加密)

crypto map BRANCH\_Map 10 ipsec-isakmp (配置加密映射表)

set peer 209.165.200.226（设置对等体IP）

set transform-set BRANCH-Set （引用之前设置的IPsec的变换集）

match address 101（匹配ACL 101）

access-list 101 permit gre host 209.165.200.242 host 209.165.200.226（建立一个对GRE的ACL）

interface Tunnel0（建GRE隧道）

ip address 172.16.100.2 255.255.255.252

tunnel source Serial0/0/1

tunnel destination 209.165.200.226

interface Serial0/0/1

crypto map BRANCH\_Map（挂接映射表）

**HQ路由器ipsec VPN配置举例：**

crypto isakmp policy 100

encryption aes

authentication pre-share

group 5

crypto isakmp key cisco address 209.165.200.242

crypto ipsec transform-set HQ-Set esp-aes esp-sha-hmac

access-list 101 permit gre host 209.165.200.226 host 209.165.200.242

crypto map HQ\_Map 10 ipsec-isakmp

set peer 209.165.200.242

set transform-set HQ-Set

match address 101

interface Tunnel0

ip address 172.16.100.1 255.255.255.252

tunnel source Serial0/0/1

interface Serial0/0/1

crypto map HQ\_Map

表1 路由器配置时用到的参数及名称

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | BRANCH路由器 |  | HQ路由器 |  |
| isakmp | policy | 100 | policy | 100 |
| 封装 | aes | 封装 | aes |
| authentication | 预共享 | authentication | 预共享 |
| Group | 5 | Group | 5 |
| key | cisco | key | cisco |
| ipsec | transform-set | BRANCH-Set | transform-set | HQ-Set |
| 加密算法 | esp-aes esp-sha-hmac | 加密算法 | esp-aes esp-sha-hmac |
|  | map | BRANCH\_Map 10 | map | HQ\_Map 10 |
|  | match address | 101 | match address | 101 |