某公司网络拓扑区域划分为母公司Site1，子公司Site2。子母公司网络通过tunnel隧道在 公网Internet打通路由。

Site1：

1、site1的部门Office1和Office2分别隶属于vlan10、vlan20，网关分别指向switch1的svi10、 svi20接口。

2、switch1和边界路由器R1之间启用动态路由协议ospf，并在区域0中宣告所有本地路由。

Site2：

1、site2的部门Office3和Office4分别隶属于vlan30、vlan40。

2、 switch2、switch3起Trunk放行vlan，并分别与边界路由器R2建立ospf邻居，在区域0中宣告所有本地直连路由。

Tunnel

1、在r1、r2上起tunnel0，源目的地址分别为自己和对端的串口。

2、 r1、r2通过tunnel隧道建立ospf邻居。

Natp+Acl：

1、 在r2上lo0口模拟公网ip：8.8.8.8。

2、r1作为Site1唯一网络出口默认路由指向外网接口s2/0，并下发默认路由。

3、r1的s2/0上开启端口复用nat对所有来自Site1内部访问外网8.8.8.8的流量进行地址转换

4、编写标准acl在switch2入方向放行pc3到所有目标地址的流量。

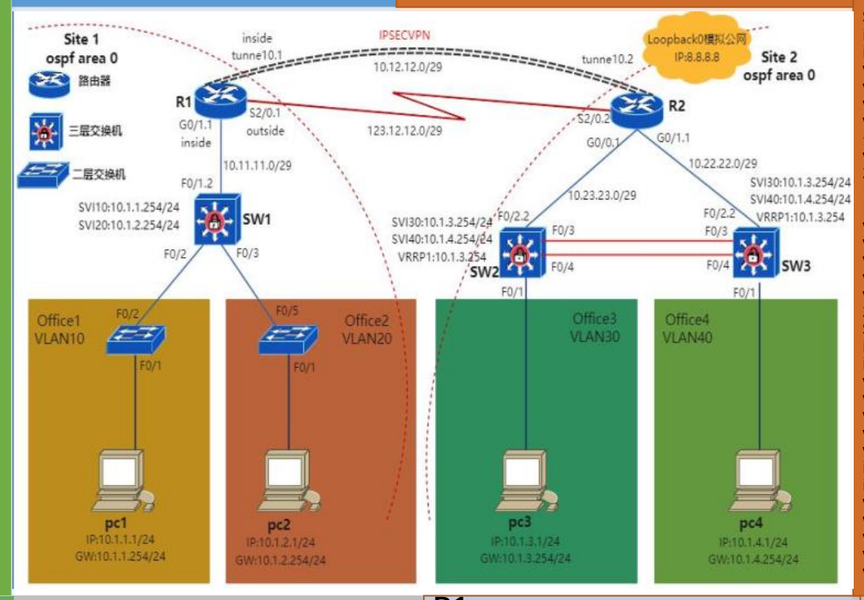
5、编写拓展acl接口下调用在switch3入方向只拒绝PC4访问8.8.8.8的流量。

SW1：

```
enable //修改主机名
configure terminal hostname switch1
spanning-tree //开启生成树
spanning-tree mode rstp
vlan 10 //创建vlan
vlan 20
interface f0/2 //划分vlan
switch mode access
switch access vlan 10
no shutdown
interface f0/3
switch mode access
switch access vlan 20
no shutdown
interface vlan 10 //进入svi口
ip address 10.1.1.254 255.255.255.0
no shutdown //打开接口
interface vlan 20 //设置svi口
ip address 10.1.2.254 255.255.255.0
no shutdown
interface f0/1 //进入接口
no switch //
关闭交换功能（打开路由功能）
ip address 10.11.11.2
255.255.255.248 //配置ip
no shutdown //开启接口
router ospf 1 //开启ospfpf进程1
network 10.1.1.0 0.0.0.255 area 0
//在area0中宣告网段10.1.1.0/24
network 10.1.2.0 0.0.0.255 area 0
network 10.11.11.0 0.0.0.7 area 0
```

信安2班

08183039	孙正雨
08183024	李徐庆
08183026	赵玉龙
08183012	李宏宇



安全配置要求:

1、在SW3·4上配置VRRP（虚拟路由冗余网关），vlan30的主虚拟网关位于SW3，vlan40的主虚拟网关位于SW4。当交换机检测上行链路转发故障时自动降低本地VRRP（路由冗余协议）优先级，虚拟网关身份切换到peer（对等）端。

2、用IPSEC（Internet协议安全）加密Tunnel隧道，模式为隧道模式。规定IKE第一阶段采用预共享密钥的方式建立安全关联，IKE第二阶段采用256位aes加密数据、sha用于数据哈希校验。

3、在SW3/4交换口上启用mac地址绑定，如果检测到主机mac改动立即关闭端口。

4、在SW1上连接到radius服务器，开启用户远程登陆的认证、授权、审计功能（RADIUS是一种用于在需要认证其链接的网络访问服务器（NAS）和共享认证服务器之间进行认证、授权和记帐信息的文档协议。RADIUS服务器负责接收用户的连接请求、认证用户，然后返回客户机所有必要的配置信息以将服务发送到用户）

VRRP（路由冗余协议）

```
SW2
int vlan 30
ip address 10.1.3.252 255.255.255.0
vrrp 1 version 2 //vrrp进程1版本2
vrrp 1 ip 10.1.3.254 //虚拟网关10.1.3.254
vrrp 1 prio 100 //本地进程优先级100（主）
vrrp 1 preempt //
开启抢占，进程优先级高的会抢占成为主设备
vrrp 1 track f0/2 20 //监控f0/
2状态，如果异常优先级降低20
Int vlan40
Ip add 10.1.4.252 255.255.255.0
vrrp 2 version 2 //进程1版本2
vrrp 2 ip 10.1.4.254 //虚拟网关10.1.4.254
vrrp 2 prio 99 //本地进程优先级99（备）
vrrp 2 preEmpt //开启抢占
vrrp 2 track f0/2 20 /监控f0/
2口状态，异常降低优先级
SW3:
int vlan 30
ip address 10.1.3.253 255.255.255.0
vrrp 1 version 2 //版本
vrrp 1 ip 10.1.3.254 //虚拟网关
vrrp 1 prio 99 //优先级（备）
vrrp 1 pre //抢占
vrrp 1 track f0/2 20 //监控端口
int vlan 40
ip add 10.1.4.253 255.255.255.0
vrrp 2 version 2 //版本
vrrp 2 ip 10.1.4.254 //虚拟网关
vrrp 2 prio 100 //优先级（主）
vrrp 2 pre //抢占
vrrp 2 track f0/2 20 //监控端口
```

IPsec（Internet 协议安全）

```
R1:
ip access-list extend 100 //拓展ACL抓取加密感兴趣流
access-list 100 permit ip 10.0.0.0 0.0.0.255 any
crypto iskamp police 10 //ike第一阶段 策略10
encry 3des //加密算法3des
authen preshare //协商方法预共享密钥
group 2 //密钥长度1024
crypto iskamp key 7 ruijie add 10.12.12.2 // 加密的共享密钥
ruijie，对端ip10.12.12.2
crypto ipsec transform-set IPSEC esp-aes-256 esp-sha-hmac
//ike第二阶段
设置传输集IPSEC，约定esp协议封装数据包、加密算法256位aes、哈希算法sha
mode tunnel //加密模式位传输
crypto map VPN 1 ipsec-iskamp //
配置加密映射表VPN策略1
set transform-set IPSEC //设定传输集IPSEC
set peer 10.12.12.2 //设置对端ip10.12.12.2
match add 100 //匹配感兴趣流量
int tunnel0
crypto map VPN //接口下调用加密策略
R2:
ip access-list extend 100 //同上
access-list 100 permit ip 10.0.0.0 0.0.0.255 any
crypto iskamp police 10
encry 3des
authen preshare
group 2
crypto iskamp key 7 ruijie add 10.12.12.1
crypto ipsec transform-set IPSEC esp-aes-256 esp-sha-hmac mode tunnel
crypto map VPN 1 ipsec-iskamp
set transform-set IPSEC
set peer 10.12.12.1
match add 100
int tunnel0
crypto map VPN
```

Port-security(交换机端口安全) SW2/SW3:

```
interface f0/2 sw port-sec mac-address sticky //
端口安全自动绑定mac
sw port-sec violation shutdown //发生违规自动关闭端口
```

AAA

```
aaa new-mode //开启AAA
radius-server hostnamest 150.1.1.1 //AAA服务器ip
radius-server key ruijie //
用于连接radius服务器的密钥ruijie
aaa authenticaton login ruijie group radius local
//
登录方法认证列表ruijie，优先采用radius组认证其次本地组
aaa local authentication attempts 3 //允许3次登录失败
aaa local authentication lockout-time 1 //
连续3次输错密码锁定账户1小时
username admin password ruijie //
创建本地用户admin密码ruijie
username admin privilege 15 //用户权限15级
aaa authostnamerization exec execauth group radius local
//
登陆授权列表execauth，优先采用radius组认证其次本地组
aauthostnamerization commands 15 commauth group radius local
//
命令授权列表commauth，优先采用radius组认证其次本地组
aaa accounting exec execaccount start-stop group radius local
//
登入登出审计列表execaccount，优先采用radius组认证其次本地组
aaa accounting commands 15 commaccount start-stop group radius
local
//
命令审计列表commaccount，优先采用radius组认证其次本地组
line vty 0 4 //进入接口vty
login authentication ruijie //接口下调用认证列表
login authostnamerization exec execauth //
接口下调用登陆授权列表
login authostnamerization commands commauth //
接口下调用命令授权列表
accouting exec execaccout //
接口下调用登入登出审计列表
accouting commands 15 commaccout //
接口下调用命令登出审计列表
```

SW2：

```
enable //修改主机名
configure terminal
hostname switch2
vlan 30 //创建vlan
vlan 40
interface vlan 30
ip address 10.1.3.254 255.255.255.0
no shutdown
interface r f0/3-4
switch mode trunk
no shutdown
interface f0/1 //vlan划分
switch mode access
switch access vlan 30
no shutdown
spanning-tree //开启生成树
spanning-tree mode mst //
生成树模式
spanning-tree mst conf //配置mst
instance 1 vlan 30 //
划分vlan30到mst实例1
instance 2 vlan 40
spanning-tree mst 1 prio 0
spanning-tree mst 2 prio 4096
interface f0/2 //
no switch //关闭交换功能配置三层ip
ip address 10.22.22.2
255.255.255.248
no shutdown
outer ospf 1
network 10.22.22.0 0.0.0.7 area 0
network 10.1.3.0 0.0.0.255 area 0
network 10.1.4.0 0.0.0.255 area 0
ip access-list stand 10 //
标准的访问控制列表10
permit hostnamet 10.1.3.1
interface f0/1 //进入接口
ip access-group 10 in
```

SW3：

```
enable //修改主机名
configure terminal
hostname switch3
vlan 30 //
vlan 40 //创建vlan40并设置svi40接口
interface vlan 40
ip address 10.1.4.254 255.255.255.0
no shutdown
interface r f0/3-4
switch mode trunk
no shutdown
interface f0/1 //vlan划分
switch mode access
switch access vlan 40
no shutdown
spanning-tree //配置mst生成树
spanning-tree mode mst
spanning-tree mst conf
instance 2 vlan 40
instance 1 vlan 30
spanning-tree mst 2 prio 0
spanning-tree mst 1 prio 4096
nterface f0/2 //
关闭交换功能，打开路由功能
no switch
ip address 10.23.23.2 255.255.255.248
no shutdown
router ospf 1 //
开启ospfpf进程1并宣告网段
network 10.23.23.0 0.0.0.7 area 0
network 10.1.4.0 0.0.0.255 area 0
network 10.1.3.0 0.0.0.255 area 0
ip access-list extenabled 100 //
拓展访问控制列表100
deny ip hostnamet 10.1.4.1 host 8.8.8.8
permit ip any any //放行所有流量
interface f0/1
ip access-group 100 in
```

SW12：

```
enable //进入特权模式修改主机名
configure terminal
hostname switch12
vlan 20 //创建vlan
spanning-tree //开启生成树
spanning-tree mode rst
interface f0/1 //划分vlan
switch mode access
switch access vlan 20
no shutdown
interface f0/2 //划分vlan
switch mode access
switch access vlan 20
no shutdown
```

SW11:

```
enable
configure terminal //特权模式
hostname switch11 //命名
vlan 10 //创建vlan10
spanning-tree //开启生成树
spanning-tree mode rstp //
设置生成树模式rstp
interface f0/1 //进入接口
switch mode access //设置接口模式
switch access vlan 10 //给接口划分vlan
no shutdown //打开接口
interface f0/2 //划分vlan
switch mode access
switch access vlan 10
no sh
```

R1：

```
enable
configure terminal
hostname R1
interface gi0/1 //给接口配置ip
ip address 10.11.11.1 255.255.255.248
no shutdown
interface s2/0
ip address 123.12.12.1 255.255.255.248
no shutdown
interface tunnel 0 //
配置tunnel口，设置模式、协议、IP地址、源目
tunnel mode gre ip
tunnel source 123.12.12.1
tunnel destination 123.12.12.2
ip address 10.12.12.1 255.255.255.248
no shutdown
router ospf 1 //ospfpf进程1
network 10.11.11.0 0.0.0.7 area 0 //
宣告接口
network 10.12.12.0 0.0.0.7 area 0
default-info originate //
给邻居下发默认路由
ip route 0.0.0.0 0.0.0.0 ser2/0 //
配置静态默认路由
ip access-list extend NAT //拓展ACl NAT
permit ip 10.1.0.0 0.0.255.255 hostnamet 8.8.8.8 //
允许源自10.1.0.0/
16的ip层流量访问主机8.8.8.8
exi //退出
ip nat inside source list NAT interface s2/0 overload //
动态nat在s2/0接口端口复用
interface s2/0
ip nat outside //nat流量为出方向
interface tunnel0
ip nat inside //nat流量进方向
interface gi0/1
ip nat inside //nat流量进方向
```

R2：

```
enable
configure terminal
hostname R2
interface gi0/0 //打开接口配置ip
ip address 10.22.22.1 255.255.255.248
no shutdown
interface gi0/1
ip address 10.23.23.1 255.255.255.248
no shutdown
interface s2/0
ip address 123.12.12.2 255.255.255.248
no shutdown
interface tunnel 0 //进入tunnel口0
tunnel mode gre ip //
tunnel模式为gre，ip支持ipv4
tunnel source 123.12.12.2 //
设置tunnel源
tunnel destination 123.12.12.1
ip address 10.12.12.2
255.255.255.248 //
给tunnel口配置ip地址
no shutdown //开启接口
interface lo 0 //进入环回接口loopback0
ip address 8.8.8.8 255.255.255.255 //
配置ip
router ospf 1 //ospfpf进程1
network 10.22.22.0 0.0.0.7 area 0 //
在areaa 0 宣告路由
network 10.23.23.0 0.0.0.7 area 0
network 10.12.12.0 0.0.0.7 area 0
```