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 隧道在在公网 interfaceernetwork 打通路由。按要求完成以下网络部署。

## 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 ospfPF，并在区域 0 中宣告所有本地路由。
**验证：**位于不同部门的 pc1、pc2 互通，R1 与 switch1 建立路由邻居并收到 vlan10、20 的路由明细。

## 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 ospfpf 邻居，在区域 0 中宣告所有本地直连路由。
**验证：**位于不同部门的 pc3、pc4 互通，R2 与 switch2、switch3 建立 ospfpf 邻居并收到 vlan30、40 的路由明细。

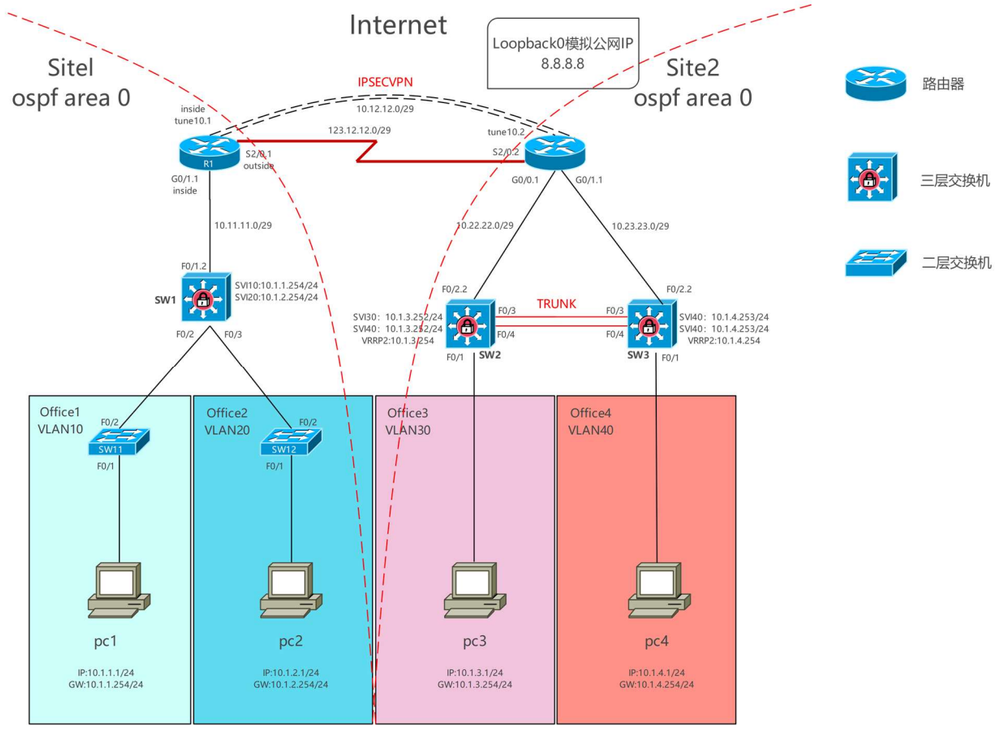
## tunnel

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 ospfpf 邻居。
**验证：**tunnel 口创建成功，r1、r2 建立 ospfpf 邻居，site1、site2 互传路由明细，pc1、pc2、pc3、pc4 四个部门互通。

## 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。
**验证：**所有 pc 互通；除 pc4 均能访问公网地址 8.8.8.8；site1 去往外部的流量实现 natp 转换。

# 网络系统与安全实践拓扑图




## SW1

```
enable //修改主机名
configure terminal
hostname switch1
spanning-treenableing-tree //开启生成树
spanning-treenableing-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 //设置 svi 的 ip 地址
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 area 0 中宣告网段 10.1.1.0/24
network 10.1.2.0 0.0.0.255 area 0 //宣告网段 10.1.1.0/24
network 10.11.11.0 0.0.0.7 area 0 //宣告网段 10.11.11.0/29
```

## 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 mst
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 //配置实例 1 优先级（本地最高）
spanning-tree mst 2 prio 4096 //配置实例 2 优先级
interface f0/2 //关闭交换功能配置三层 ip
no switch
ip address 10.22.22.2 255.255.255.248
no shutdown
router ospf 1 //开启 ospfpf 进程并在 areaa 0 中宣告路由
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 //放行源地址是 10.1.3.1 的所有流量
interface f0/1 //进入接口
ip access-group 10 in //将 ACL10 接口下调用在接口的入方向
```

## 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
interface 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
//拒绝主机 10.1.4.1 访问主机 8.8.8.8
permit ip any any //放行所有流量
interface f0/1 //进入接口 f0/1 并在入方向接口下调用 ACL100
ip access-group 100 in
```

## 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
```

## 安全配置：

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 进程优先级，虚拟网关身份切换到 peer 端。
2、用 IPSEC 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。

## 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 shutdown
```

## 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 rstp
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
```

## 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 //设置 tunnel 目的
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
```

## VRRP

### 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

### R1

```
ip access-list extend 100 //拓展 ACL 抓取加密感兴趣流
per ip 10.0.0.0 0.0.0.255
crypto iskamp police 10 //ike 第一阶段策略 10
encry 3des //加密算 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
per ip 10.0.0.0 0.0.0.255
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
```

## MAC 地址绑定

### SW2

```
interface f0/1
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
```

### SW3

```
interface f0/1
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：

### SW1：

```
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
```


信安 19-1 08193035 朱公澳
信安 19-1 08193028 周炯超
信安 19-1 08193041 江一川
信安 19-1 08192945 邹凯蓄