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（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

//per ip 10.0.0.0 0.0.0.255 老师提供的 有问题

access-list 100 permit ip 10.0.0.0 0.0.0.255 any // conf模式 修改后命令

crypto iskamp policy 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

// per ip 10.0.0.0 0.0.0.255 老师提供的 有问题

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