 各网络设备均开启SSH服务，用户名密码分别为admin、ruijie123，特权密码为ruijie123；

R1：

FZ2-RSR20-R1(config)#username admin password ruijie123

FZ2-RSR20-R1(config)#enable service ssh-server

FZ2-RSR20-R1(config)#enable password ruijie123

FZ2-RSR20-R1(config)#line vty 0 4

FZ2-RSR20-R1(config-line)#login local

FZ2-RSR20-R1(config-line)#transport in ssh

FZ2-RSR20-R1(config-line)#exit

 管理员计划增设网管平台，平台IP规划为172.16.0.254，为了网管平台后期上线后可用，需要在每台设备上部署SNMP功能。配置所有设备SNMP消息，向主机172.16.0.254发送Trap消息版本采用V2C，读写的Community为“ruijie”，只读的Community为“public”，开启Trap消息。

R1:

FZ2-RSR20-R1(config)#snmp-server host 172.16.0.254 traps version 2c ruijie

FZ2-RSR20-R1(config)#snmp-server host 172.16.0.254 traps version 2c public

FZ2-RSR20-R1(config)#snmp-server enable traps

FZ2-RSR20-R1(config)#snmp-server community ruijie rw

FZ2-RSR20-R1(config)#snmp-server community public ro

1. **MSTP及VRRP部署**

在交换机S1、S2、S3、S4上配置MSTP防止二层环路；要求VLAN10、VLAN20数据流经过S3转发，S3失效时经过S4转发；VLAN50、VLAN60、VLAN100数据流经过S4转发，S4失效时经过S3转发。所配置的参数要求如下：

* region-name为ruijie；
* revision版本为1；
* 实例1包含VLAN10,VLAN20；
* 实例2包含VLAN50,VLAN60,VLAN100；
* S3作为实例1的主根、实例2的从根， S4作为实例2的主根、实例1的从根；
* 主根优先级为4096，从根优先级为8192；

例S4配置：

FZ1-S5750-S4(config)#spanning-tree mst configuration

FZ1-S5750-S4(config-mst)# revision 1

FZ1-S5750-S4(config-mst)# name ruijie

FZ1-S5750-S4(config-mst)# instance 1 vlan 10, 20

%Warning:you must create vlans before configuring instance-vlan relationship.

FZ1-S5750-S4(config-mst)# instance 2 vlan 50, 60, 100

%Warning:you must create vlans before configuring instance-vlan relationship.

FZ1-S5750-S4(config)#spanning-tree mst 1 priority 8192

FZ1-S5750-S4(config)#spanning-tree mst 2 priority 4096

FZ1-S5750-S4(config)#spanning-tree

Enable spanning-tree.

* S3、S4连接接入交换机S1、S2的接口启用TC-IGNORE功能，规避接入设备频繁的网络震荡；

FZ1-S5750-S4(config)#interface GigabitEthernet 0/1

FZ1-S5750-S4(config-if-GigabitEthernet 0/1)# spanning-tree ignore tc

FZ1-S5750-S4(config-if-GigabitEthernet 0/1)#interface GigabitEthernet 0/2

FZ1-S5750-S4(config-if-GigabitEthernet 0/2)# spanning-tree ignore tc:

FZ1-S5750-S4(config-if-GigabitEthernet 0/2)#exi

* 在S3和S4上配置VRRP，实现主机的网关冗余，所配置的参数要求如表11；
* S3、S4各VRRP组中高优先级设置为150，低优先级设置为120。

FZ1-S5750-S4(config)#int vlan 10

FZ1-S5750-S4(config-if-VLAN 10)# vrrp 10 ip 192.1.10.254

FZ1-S5750-S4(config-if-VLAN 10)# vrrp 10 priority 120

FZ1-S5750-S4(config-if-VLAN 10)#int vlan 20

FZ1-S5750-S4(config-if-VLAN 20)# vrrp 20 ip 192.1.20.254

FZ1-S5750-S4(config-if-VLAN 20)# vrrp 20 priority 120

FZ1-S5750-S4(config-if-VLAN 20)#int vlan 50

FZ1-S5750-S4(config-if-VLAN 50)# vrrp 50 ip 192.1.50.254

FZ1-S5750-S4(config-if-VLAN 50)# vrrp 50 priority 150

FZ1-S5750-S4(config-if-VLAN 50)#int vlan 60

FZ1-S5750-S4(config-if-VLAN 60)# vrrp 60 ip 192.1.60.254

FZ1-S5750-S4(config-if-VLAN 60)# vrrp 60 priority 150

FZ1-S5750-S4(config-if-VLAN 60)#int vlan 100

FZ1-S5750-S4(config-if-VLAN 100)# vrrp 100 ip 192.1.100.254

FZ1-S5750-S4(config-if-VLAN 100)# vrrp 100 priority 150

FZ1-S5750-S4(config-if-VLAN 100)#exi

* 为提升冗余性，交换机S3与S4之间的2条互联链路（Gi0/22、Gi0/23）配置二层链路聚合，采取LACP动态聚合模式。

FZ1-S5750-S4(config)#int aggregatePort 1

FZ1-S5750-S4(config-if-AggregatePort 1)#switchport mode trunk

FZ1-S5750-S4(config-if-AggregatePort 1)#switchport trunk allowed vlan 10,20,50,60,100

FZ1-S5750-S4(config-if-AggregatePort 1)#exi

FZ1-S5750-S4(config)#int r gi0/22 -23

FZ1-S5750-S4(config-if-range)#port-group 1 mode active

1. **DHCP中继与服务安全部署**

在交换机S3、S4上配置DHCP中继，对局域网的终端进行地址中继，使得终端用户使用DHCP Relay方式获取IP地址。具体要求如下：

* DHCP服务器搭建于EG1上，DHCP对外服务使用loopback 0地址；

EG1配置：

FZ1-EG2000-EG1(config)#ip dhcp excluded-address 192.1.60.252 192.1.60.254

FZ1-EG2000-EG1(config)#ip dhcp excluded-address 192.1.50.252 192.1.50.254

FZ1-EG2000-EG1(config)#ip dhcp pool AP

FZ1-EG2000-EG1(dhcp-config)#option 138 ip 10.2.1.6

FZ1-EG2000-EG1(dhcp-config)#network 192.1.50.0 255.255.255.0

FZ1-EG2000-EG1(dhcp-config)#default-router 192.1.50.254

FZ1-EG2000-EG1(dhcp-config)#exi

FZ1-EG2000-EG1(config)#ip dhcp pool yonghu

FZ1-EG2000-EG1(dhcp-config)#network 192.1.60.0 255.255.255.0

FZ1-EG2000-EG1(dhcp-config)#default-router 192.1.60.254

FZ1-EG2000-EG1(dhcp-config)#exi

S3/S4配置：

FZ1-S5750-S4(config)#service dhcp

FZ1-S5750-S4(config)#ip helper-address 10.1.0.1

为了减少网络广播，需要规划和配置VLAN，要求如下：

 配置合理，Trunk链路上不允许不必要VLAN的数据流通过；

 为隔离终端间的二层互访，在交换机S1、S2的Gi0/1-Gi0/22端口启用端口保护；

S1:

FZ1-S2910-S1(config)#int r gi0/1-22

FZ1-S2910-S1(config-if-range)#switchport protected

interface GigabitEthernet 0/21

switchport protected

switchport mode trunk

switchport trunk native vlan 50

switchport trunk allowed vlan only 50,60

!

interface GigabitEthernet 0/22

switchport protected

switchport mode trunk

switchport trunk allowed vlan only 60,100

!

interface GigabitEthernet 0/23

switchport mode trunk

switchport trunk allowed vlan only 10,20,50,60,100

!

interface GigabitEthernet 0/24

switchport mode trunk

switchport trunk allowed vlan only 10,20,50,60,100

S2:

FZ1-S2910-S2(config)#int r gi0/1-22

FZ1-S2910-S2(config-if-range)#switchport protected

interface GigabitEthernet 0/21

switchport protected

switchport mode trunk

switchport trunk native vlan 50

switchport trunk allowed vlan only 50,60

!

interface GigabitEthernet 0/22

switchport protected

switchport mode trunk

switchport trunk allowed vlan only 60,100

!

interface GigabitEthernet 0/23

switchport mode trunk

switchport trunk allowed vlan only 10,20,50,60,100

!

interface GigabitEthernet 0/24

switchport mode trunk

switchport trunk allowed vlan only 10,20,50,60,100

局域网环路规避方案部署

为规避网络末端接入设备上出现环路影响全网，要求在接入设备S1、S2进行防环处理。具体要求如下：

 连接PC端口开启Portfast和BPDUguard防护功能；

 为防止接入交换机下联端口私接HUB设备引起环路，需要启用RLDP协议；

 终端接口检测到环路后处理方式为 Shutdown-Port；

 端口检测进入 Err-Disabled状态，设置 300 秒自动恢复机制（基于接口部署策略）

S1:

FZ1-S2910-S1(config)#int r gi0/1-20

FZ1-S2910-S1(config-if-range)#spanning-tree bpduguard enable

FZ1-S2910-S1(config-if-range)# ip verify source port-security

FZ1-S2910-S1(config-if-range)# spanning-tree portfast

FZ1-S2910-S1(config-if-range)#rldp port loop-detect shutdown-port

FZ1-S2910-S1(config-if-range)#errdisable recovery interval 300

FZ1-S2910-S1(config-if-range)#exit

FZ1-S2910-S1(config)#rldp enable

S2:

FZ1-S2910-S2(config)#int r gi0/1-20

FZ1-S2910-S2(config-if-range)#spanning-tree bpduguard enable

FZ1-S2910-S2(config-if-range)#rldp port loop-detect shutdown-port

FZ1-S2910-S2(config-if-range)#errdisable recovery interval 300

FZ1-S2910-S1(config-if-range)# ip verify source port-security

FZ1-S2910-S1(config-if-range)# spanning-tree portfast

FZ1-S2910-S2(config-if-range)#exit

FZ1-S2910-S2(config)#rldp enable

 为了防御局域网伪造DHCP服务器与ARP欺骗，在S1、S2交换机部署DHCP Snooping+DAI功能，DAI针对VLAN10与VLAN20启用ARP防御；

S1:

FZ1-S2910-S1(config)# ip dhcp snooping

FZ1-S2910-S1(config)#ip arp inspection vlan 10

FZ1-S2910-S1(config)#ip arp inspection vlan 20

FZ1-S2910-S1(config)#int r gi0/23-24

FZ1-S2910-S1(config-if-range)#ip dhcp snooping trust

FZ1-S2910-S1(config-if-range)#ip arp inspection trust

S2:

FZ1-S2910-S2(config)#service dhcp

FZ1-S2910-S2(config)#ip arp inspection vlan 10

FZ1-S2910-S2(config)#ip arp inspection vlan 20

FZ1-S2910-S2(config)#int r gi0/23-24

FZ1-S2910-S2(config-if-range)#ip dhcp snooping trust

FZ1-S2910-S2(config-if-range)#ip arp inspection trust

 为了防止大量网关发送的正常的相关报文被接入交换机误认为是攻击被丢弃，从而导致下联用户无法获取网关的ARP信息而无法上网，要求关闭S1/S2上联口的NFPP arp-guard功能；

S1:

FZ1-S2910-S1(config)#int r gi0/23-24

FZ1-S2910-S1(config-if-range)#no nfpp nd-guard enable

S2:

FZ1-S2910-S2(config)#int r gi0/23-24

FZ1-S2910-S2(config-if-range)#no nfpp nd-guard enable

 调整S1、S2设备CPU保护机制中ARP带宽为1000pps。

S1:

FZ1-S2910-S1(config)#cpu-protect type arp bandwidth 1000

S2:

FZ1-S2910-S2(config)#cpu-protect type arp bandwidth 1000

* 规划S6和S7间的Te0/49-50端口作为VSL链路，使用VSU技术实现网络设备虚拟化。其中S6为主，S7为备；
* 规划S6和S7间的Gi0/47端口作为双主机检测链路，配置基于BFD的双主机检测，当VSL的所有物理链路都异常断开时，备机会切换成主机，从而保障网络正常；
* 主设备：Domain id：1,switch id:1,priority 150, description: S6000-1；
* 备设备：Domain id：1,switch id:2,priority 120, description: S6000-2。

主设备：

Ruijie(config)#switch virtual domain 1

Ruijie(config-vs-domain)#switch 1 priority 150

Ruijie(config-vs-domain)#switch 1 description S6000-1

Ruijie(config-vs-domain)#exi

Ruijie(config)#vsl-port

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/49

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/50

Ruijie(config-vsl-port)#end

\*Jun 22 09:53:29: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#

Ruijie#wr

Ruijie#switch convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

备设备：

Ruijie(config)#switch virtual domain 1

Ruijie(config-vs-domain)#switch 2 priority 120

Ruijie(config-vs-domain)#switch 2 description S6000-2

Ruijie(config-vs-domain)#exi

Ruijie(config)#vsl-port

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/49

Ruijie(config-vsl-port)#port-member interface tenGigabitEthernet 0/50

Ruijie(config-vsl-port)#end

\*Jun 22 09:53:29: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#

Ruijie#wr

Ruijie#switch convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

BFD检测：

Ruijie (config)#int r gi1/0/47 , 2/0/47

Ruijie (config-if-range)#no switchport

Ruijie (config-if-range)#exi

Ruijie (config)#switch virtual domain 1

Ruijie (config-vs-domain)#dual-active detection bfd

Ruijie (config-vs-domain)# dual-active bfd interface gigabitEthernet 1/0/47

Ruijie (config-vs-domain)# dual-active bfd interface gigabitEthernet 2/0/47

1. **AC冗余部署**

* 为了提升冗余性，两台AC使用虚拟化方案VAC技术组合成1台虚拟AC；
* 规划AC1和AC2间的Gi0/4-5端口作为VSL链路，其中AC1为主，AC2为备；
* 规划AC1和AC2间的Gi0/3端口作为双主机检测链路，配置基于BFD的双主机检测，当VSL的所有物理链路都异常断开时，备机会切换成主机，从而保障网络正常；
* 主设备：Domain id：1,device id:1,priority 150, description: AC-1;
* 备设备：Domain id：1,device id:2,priority 120, description: AC-2；

主设备：

Ruijie(config)#virtual-ac domain 1

Ruijie(config-vac-domain)#device 1 priority 150

Ruijie(config-vac-domain)#device 1 description AC-1

Ruijie(config-vac-domain)#exi

Ruijie(config)#vac-port

Ruijie(config-vac-port)#port-member interface gigabitEthernet 0/4

Ruijie(config-vac-port)#port-member interface gigabitEthernet 0/5

Ruijie(config-vac-port)#exi

Ruijie(config)#end

\*Jun 23 10:48:10: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#wr

Ruijie#device convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

备设备：

Ruijie(config)#virtual-ac domain 1

Ruijie(config-vac-domain)#device 2 priority 120

Ruijie(config-vac-domain)#device 2 description AC-2

Ruijie(config-vac-domain)#exi

Ruijie(config)#vac-port

Ruijie(config-vac-port)#port-member interface gigabitEthernet 0/4

Ruijie(config-vac-port)#port-member interface gigabitEthernet 0/5

Ruijie(config-vac-port)#end

\*Jun 23 10:51:45: %SYS-5-CONFIG\_I: Configured from console by console

Ruijie#wr

Ruijie#device convert mode virtual

Convert mode will backup and delete config file, and reload the switch. Are you sure to continue[yes/no]:y

BFD检测：

Ruijie(config)#int r gi1/0/3 , 2/0/3

Ruijie(config-if-range)#no switchport

Ruijie(config-if-range)#exi

Ruijie(config)#virtual-ac domain 1

Ruijie(config-vac-domain)#dual-active detection bfd

Ruijie(config-vac-domain)#dual-active bfd interface gigabitEthernet 1/0/3

Ruijie(config-vac-domain)#dual-active bfd interface gigabitEthernet 2/0/3

1. **胖AP部署**

无线设备AP3使用胖模式进行部署，具体要求如下：

* AP3使用透明模式，管理地址为192.XX.100.3/24(XX现场提供)；

FZ1-AP720-AP3(config)#vlan 100

FZ1-AP720-AP3(config-vlan)#name Manage

FZ1-AP720-AP3(config-vlan)#exi

FZ1-AP720-AP3(config)#int bvI 100

FZ1-AP720-AP3(config-if-BVI 100)#ip address 192.1.100.3 24

FZ1-AP720-AP3(config)#int gi0/1.100

FZ1-AP720-AP3(config-subif-GigabitEthernet 0/1.100)#encapsulation dot1Q 100

* AP3创建 SSID(WLAN-ID 2) 为 Ruijie-Fat\_XX(XX现场提供), 内网无线用户关联SSID后可自动获取VLAN60网段地址。

FZ1-AP720-AP3(config)#dot11 wlan 2

FZ1-AP720-AP3(dot11-wlan-config)#vlan 60

FZ1-AP720-AP3(dot11-wlan-config)#ssid Ruijie-Fat\_1

FZ1-AP720-AP3(dot11-wlan-config)#exi

FZ1-AP720-AP3(config)#int gi0/1.60

FZ1-AP720-AP3(config-subif-GigabitEthernet 0/1.60)#encapsulation dot1Q 60

FZ1-AP720-AP3(config-subif-GigabitEthernet 0/1.60)#exi

FZ1-AP720-AP3(config)#int dot11radio 1/0.6

FZ1-AP720-AP3(config-subif-Dot11radio 1/0.6)#encapsulation dot1Q 60

FZ1-AP720-AP3(config-subif-Dot11radio 1/0.6)#wlan-id 2

FZ1-AP720-AP3(config-subif-Dot11radio 1/0.6)#exi

* 连接Fat AP的无线用户接入无线网络时采用WEB认证方式，认证用户名、密码为XX(现场提供)。

FZ1-AP720-AP3(config)#aaa new-model

FZ1-AP720-AP3(config)#aaa authentication iportal default local

FZ1-AP720-AP3(config)#aaa accounting network default start-stop none

FZ1-AP720-AP3(config)#http redirect direct-arp 192.1.60.254

FZ1-AP720-AP3(config)#http redirect port 8081

FZ1-AP720-AP3(config)#username user1 web-auth password user1

FZ1-AP720-AP3(config)#web-auth template iportal

FZ1-AP720-AP3(config.tmplt.iportal)#

FZ1-AP720-AP3(config.tmplt.iportal)#exi

FZ1-AP720-AP3(config)#wlansec 2

FZ1-AP720-AP3(config-wlansec)#web-auth portal iportal

FZ1-AP720-AP3(config-wlansec)#webauth

* 为了保障总部每个用户的无线体验，针对WLAN ID 2下的每个用户的下行平均速率为 800KB/s ，突发速率为1600KB/s；

FZ1-AP720-AP3(config)#wlan-qos wlan-based 2 per-user-limit down-streams average-data-rate 800 burst-data-rate 1600

* 关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

FZ1-AP720-AP3(config)#int dot11radio 1/0

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11b disable 1

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11b disable 2

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11b disable 5

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11g disable 5

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11g disable 2

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#rate-set 11g disable 1

FZ1-AP720-AP3(config-if-Dot11radio 1/0)#exi

FZ1-AP720-AP3(config)#int dot11radio 2/0

FZ1-AP720-AP3(config-if-Dot11radio 2/0)#rate-set 11a disable 6

FZ1-AP720-AP3(config-if-Dot11radio 2/0)#rate-set 11a disable 9

1. **分支机构间IPV6部署**

* 分支机构间部署IPV6网络实现机构内网IPV6终端可自动从网关处获取地址；
* IPV6地址规划如下：

**表-1**2 **IPV6地址规划表**

|  |  |  |
| --- | --- | --- |
| 设备 | 接口 | IPV6地址 |
| R1 | VLAN10 | 2001:194:1:10::254/64 |
| VLAN20 | 2001:194:1:20::254/64 |
| Tunnel0 | 2001:11:1:3::1/64 |
| VSU | VLAN10 | 2001:195:1:10::254/64 |
| VLAN20 | 2001:195:1:20::254/64 |
| Tunnel0 | 2001:11:1:3::2/64 |

例：R1配置：

FZ2-RSR20-R1(config)#int vlan 10

FZ2-RSR20-R1(config-if-VLAN 10)#ipv6 enable

FZ2-RSR20-R1(config-if-VLAN 10)#ipv6 address 2001:194:1:10::254/64

FZ2-RSR20-R1(config-if-VLAN 10)#no ipv6 nd suppress-ra

FZ2-RSR20-R1(config-if-VLAN 10)#exi

FZ2-RSR20-R1(config)#int vlan 20

FZ2-RSR20-R1(config-if-VLAN 20)#ipv6 enable

FZ2-RSR20-R1(config-if-VLAN 20)#ipv6 address 2001:194:1:20::254/64

FZ2-RSR20-R1(config-if-VLAN 20)#no ipv6 nd suppress-ra

FZ2-RSR20-R1(config-if-VLAN 20)#exi

FZ2-RSR20-R1(config)#int tunnel 0

FZ2-RSR20-R1(config-if-Tunnel 0)#ipv6 enable

FZ2-RSR20-R1(config-if-Tunnel 0)#ipv6 address 2001:11:1:3::1/64

FZ2-RSR20-R1(config-if-Tunnel 0)#tunnel source 11.1.0.1

FZ2-RSR20-R1(config-if-Tunnel 0)#tunnel destination 11.1.0.67

FZ2-RSR20-R1(config)#ipv6 router ospf 10

FZ2-RSR20-R1(config-router)#passive-interface vlan 10

FZ2-RSR20-R1(config-router)#passive-interface vlan 20

FZ2-RSR20-R1(config-router)#exi

FZ2-RSR20-R1(config)#int vlan 10

FZ2-RSR20-R1(config-if-VLAN 10)#ipv6 ospf 10 area 0

FZ2-RSR20-R1(config-if-VLAN 10)#exi

FZ2-RSR20-R1(config)#int vlan 20

FZ2-RSR20-R1(config-if-VLAN 20)#ipv6 ospf 10 area 0

FZ2-RSR20-R1(config-if-VLAN 20)#exi

FZ2-RSR20-R1(config)#int tunnel 0

FZ2-RSR20-R1(config-if-Tunnel 0)#ipv6 ospf 10 area 0

各机构内网均使用OSPF协议组网，运营商不维护EG1/EG2局域网内部网段。具体要求如下：

 VAC、S5、EG2间运行OSPF，进程号10，规划单区域：区域0；

 R1、R2、R3间运行OSPF，进程号20，规划单区域：区域0；

 VSU、R2、R3间运行OSPF，进程号21，规划单区域：区域0；

 S3、S4、EG1间运行OSPF，进程号为30；

 要求业务网段中不出现协议报文；

 R1、VSU始发的终端网段及各设备Loopback管理地址均以重分发直连的方式注入；

 R2/EG2、R3/EG1间互联段均以重发布直连的方式注入R2、R3 OSPF双进程中；

 R2、R3间启用OSPF与BFD联动以达到迅速检测运营商网络中断，快速地切换到其他备份线路，提高用户网络体验。

 优化OSPF相关配置，以尽量加快OSPF收敛；

 重发布路由进OSPF中使用类型1。

注意：S5需要重发布云平台（172.16.0.0/22）静态路由至服务区内网。

VAC:

FW-WS6008-VAC(config)#rou ospf 10

FW-WS6008-VAC(config-router)#netw 10.2.1.6 0.0.0.3 a 0

FW-WS6008-VAC(config-router)#redistribute connected subnets metric-type 1 FW-WS6008-VAC(config-router)#int agg 1

FW-WS6008-VAC(config-if-AggregatePort 1)#ip ospf ne point-to-point

S5:

FW-S5750-S5(config)#rou ospf 10

FW-S5750-S5(config-router)#network 10.2.1.2 0.0.0.3 a 0

FW-S5750-S5(config-router)#network 10.2.1.5 0.0.0.3 a 0

FW-S5750-S5(config-router)#redistribute connected subnets metric-type 1

FW-S5750-S5(config-router)#redistribute static metric-type 1 subnets

FW-S5750-S5(config)#ip rou 172.16.0.0 255.255.252.0 193.1.0.2

FW-S5750-S5(config)#int gi0/24

FW-S5750-S5(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point

FW-S5750-S5(config-if-GigabitEthernet 0/24)#int agg 1

FW-S5750-S5(config-if-AggregatePort 1)#ip ospf ne point-to-point

EG2:

FW-EG2000-EG2(config)#rou ospf 10

FW-EG2000-EG2(config-router)#network 10.2.1.1 0.0.0.3 a 0

FW-EG2000-EG2(config-router)#redistribute con metric-type 1 subnets

FW-EG2000-EG2(config-router)#default-information originate metric-type 1

FW-EG2000-EG2(config-router)#exit

FW-EG2000-EG2(config)#ip rou 0.0.0.0 0.0.0.0 11.1.1.9

FW-EG2000-EG2(config) #int gi0/1

FW-EG2000-EG2(config) # ip ospf ne point-to-point

R1:

FZ2-RSR20-R1(config)#rou ospf 20

FZ2-RSR20-R1(config-router)#network 11.1.1.1 0.0.0.3 a 0

FZ2-RSR20-R1(config-router)#network 11.1.2.1 0.0.0.3 a 0

FZ2-RSR20-R1(config-router)#int gi0/0

FZ2-RSR20-R1(config-if-GigabitEthernet 0/0)#ip ospf ne point-to-point

FZ2-RSR20-R1(config-if-GigabitEthernet 0/0)#int gi0/1

FZ2-RSR20-R1(config-if-GigabitEthernet 0/1)#ip ospf ne point-to-point

R2:

R3:

VSU:

FZ3-S6000C-VSU(config)#rou ospf 21

FZ3-S6000C-VSU(config-router)#netw 11.1.1.6 0.0.0.3 a 0

FZ3-S6000C-VSU(config-router)#netw 11.1.2.6 0.0.0.3 a 0

FZ3-S6000C-VSU(config-router)#int gi1/0/48

FZ3-S6000C-VSU(config-if-GigabitEthernet 1/0/48)#ip ospf ne point-to-p

FZ3-S6000C-VSU(config-if-GigabitEthernet 1/0/48)#int gi2/0/48

FZ3-S6000C-VSU(config-if-GigabitEthernet 2/0/48)#ip ospf ne point-to-p

S3:

FZ1-S5750-S3(config)#rou ospf 30

FZ1-S5750-S3(config-router)#network 10.1.1.2 0.0.0.3 a 0

FZ1-S5750-S3(config-router)#network 192.1.10.0 0.0.0.255 a 0

FZ1-S5750-S3(config-router)#network 192.1.20.0 0.0.0.255 a 0

FZ1-S5750-S3(config-router)#network 192.1.50.0 0.0.0.255 a 0

FZ1-S5750-S3(config-router)#network 192.1.60.0 0.0.0.255 a 0

FZ1-S5750-S3(config-router)#network 192.1.100.0 0.0.0.255 a 0

FZ1-S5750-S3(config-router)#passive-interface vlan 10

FZ1-S5750-S3(config-router)#passive-interface vlan 20

FZ1-S5750-S3(config-router)#passive-interface vlan 50

FZ1-S5750-S3(config-router)#passive-interface vlan 60

FZ1-S5750-S3(config-router)#redistribute connected metric-type 1 subnets

FZ1-S5750-S3(config-router)#int gi0/24

FZ1-S5750-S3(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point

FZ1-S5750-S3(config-if-GigabitEthernet 0/24)#int vlan 100

FZ1-S5750-S3(config-if-VLAN 100)#ip ospf ne point-to-point

S4:

FZ1-S5750-S4(config)#rou ospf 30

FZ1-S5750-S4(config-router)#network 10.1.1.6 0.0.0.3 a 0

FZ1-S5750-S4(config-router)#network 192.1.10.0 0.0.0.255 a 0

FZ1-S5750-S4(config-router)#network 192.1.20.0 0.0.0.255 a 0

FZ1-S5750-S4(config-router)#network 192.1.50.0 0.0.0.255 a 0

FZ1-S5750-S4(config-router)#network 192.1.60.0 0.0.0.255 a 0

FZ1-S5750-S4(config-router)#network 192.1.100.0 0.0.0.255 a 0

FZ1-S5750-S4(config-router)#passive-interface vlan 10

FZ1-S5750-S4(config-router)#passive-interface vlan 20

FZ1-S5750-S4(config-router)#passive-interface vlan 50

FZ1-S5750-S4(config-router)#passive-interface vlan 60

FZ1-S5750-S4(config-router)#redistribute connected metric-type 1 subnets

FZ1-S5750-S4(config-router)#int gi0/24

FZ1-S5750-S4(config-if-GigabitEthernet 0/24)#ip ospf ne point-to-point

FZ1-S5750-S4(config-if-GigabitEthernet 0/24)#int vlan 100

FZ1-S5750-S4(config-if-VLAN 100)#ip ospf ne point-to-point

EG1:

FZ1-EG2000-EG1(config)#rou ospf 30

FZ1-EG2000-EG1(config-router)#network 10.1.1.1 0.0.0.3 a 0

FZ1-EG2000-EG1(config-router)#network 10.1.1.5 0.0.0.3 a 0

FZ1-EG2000-EG1(config-router)#re con metric-type 1 subnets

FZ1-EG2000-EG1(config-router)#default-information originate metric-type 1

FZ1-EG2000-EG1(config-router)#int gi0/1

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/1)#ip ospf ne point-to-point

FZ1-EG2000-EG1(config-router)#int gi0/2

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/1)#ip ospf ne point-to-point

考虑到数据分流及负载均衡的目的进行路由策略部署，具体要求如下：

 R1引入路由时进行路由标记，生产网段标记为10，办公网段标记为20，loopback地址标记为30，路由图定义为SET\_TAG；

R1:

FZ2-RSR20-R1(config)#route-map SET\_TAG permit 10

FZ2-RSR20-R1(config-route-map)#match interface vlan 10

FZ2-RSR20-R1(config-route-map)#set tag 10

FZ2-RSR20-R1(config-route-map)#exit

FZ2-RSR20-R1(config)#route-map SET\_TAG permit 20

FZ2-RSR20-R1(config-route-map)#match interface vlan 20

FZ2-RSR20-R1(config-route-map)#set tag 20

FZ2-RSR20-R1(config-route-map)#exit

FZ2-RSR20-R1(config)#route-map SET\_TAG permit 30

FZ2-RSR20-R1(config-route-map)#match interface loop 0

FZ2-RSR20-R1(config-route-map)#set tag 30

FZ2-RSR20-R1(config-route-map)#exit

FZ2-RSR20-R1(config-router)#redistribute connected subnets metric-type 1 route -map SET\_TAG

 VSU引入路由时进行路由标记，生产网段标记为100，办公网段标记为200，loopback地址标记为300，路由图定义为SET\_TAG；

VSU:

FZ3-S6000C-VSU(config)#route-map SET\_TAG permit 10

FZ3-S6000C-VSU(config-route-map)#match interface vlan 10

FZ3-S6000C-VSU(config-route-map)#set tag 100

FZ3-S6000C-VSU(config-route-map)#exit

FZ3-S6000C-VSU(config)#route-map SET\_TAG permit 20

FZ3-S6000C-VSU(config-route-map)#match interface vlan 20

FZ3-S6000C-VSU(config-route-map)#set tag 200

FZ3-S6000C-VSU(config-route-map)#exit

FZ3-S6000C-VSU(config)#route-map SET\_TAG permit 30

FZ3-S6000C-VSU(config-route-map)#match interface loop 0

FZ3-S6000C-VSU(config-route-map)#set tag 300

FZ3-S6000C-VSU(config-route-map)#exit

FZ3-S6000C-VSU(config)#rou ospf 21

FZ3-S6000C-VSU(config-router)#redistribute connected subnets metric-type 1 route-map SET\_TAG

 R2、R3要求OSPF双进程重发布,OSPF20进程发布至OSPF21进程时关联路由图定义为OSPF20\_TO\_OSPF21，OSPF21进程发布至OSPF20进程时关联路由图定义为OSPF21\_TO\_OSPF20；

 R2、R3要求OSPF路由标记过滤规避路由环路与次优路径风险，OSPF20进程内路由过滤关联路由图定义为FILTER\_OSPF21\_TAG，OSPF21进程内路由过滤关联路由图定义为FILTER\_OSPF20\_TAG；

 路由图中涉及COST值的调整，要求其值必须为5或10；

 通过策略部署，使得生产业务的主路径为R1—R2—VSU,办公业务的主路径为R1—R3—VSU，且要求来回路径一致。Loopback接口互访路径与办公业务一致；

 主链路或R2、R3故障时可无缝切换到备用链路上。

R3:

R3(config)#route-map OSPF20\_TO\_OSPF21 permit 10

R3(config-route-map)#match tag 10

R3(config-route-map)#set metric 10

R3(config-route-map)#exit

R3(config)#route-map OSPF20\_TO\_OSPF21 permit 20

R3(config-route-map)#match tag 20

R3(config-route-map)#exit

R3(config)#route-map OSPF20\_TO\_OSPF21 permit 30

R3(config-route-map)#match tag 30

R3(config-route-map)#exit

R3(config)#route-map OSPF21\_TO\_OSPF20 permit 10

R3(config-route-map)#match tag 100

R3(config-route-map)#set metric 10

R3(config-route-map)#route-map OSPF21\_TO\_OSPF20 permit 20

R3(config-route-map)#match tag 200

R3(config-route-map)#route-map OSPF21\_TO\_OSPF20 permit 30

R3(config-route-map)#match tag 300

R3(config)#rou ospf 20

R3(config-router)#redistribute ospf 21 metric-type 1 subnets route-map OSPF21\_TO\_OSPF20

R3(config-router)#rou ospf 21

R3(config-router)#redistribute ospf 20 metric-type 1 subnets route-map OSPF20\_TO\_OSPF21

R2:

R2(config)#route-map OSPF21\_TO\_OSPF20 permit 10

R2(config-route-map)#match tag 100

R2(config-route-map)#

R2(config-route-map)#route-map OSPF21\_TO\_OSPF20 permit 20

R2(config-route-map)#match tag 200

R2(config-route-map)#set metric 10

R2(config-route-map)#route-map OSPF21\_TO\_OSPF20 permit 30

R2(config-route-map)#match tag 300

R2(config-route-map)#

R2(config-route-map)#route-map OSPF20\_TO\_OSPF21 permit 10

R2(config-route-map)#match tag 10

R2(config-route-map)#

R2(config-route-map)#route-map OSPF20\_TO\_OSPF21 permit 20

R2(config-route-map)#match tag 20

R2(config-route-map)#set metric 10

R2(config-route-map)#route-map OSPF20\_TO\_OSPF21 permit 30

R2(config-route-map)#match tag 30

R2(config)#rou ospf 20

R2(config-router)#redistribute ospf 21 metric-type 1 subnets route-map OSPF21\_TO\_OSPF20

R2(config-router)#rou ospf 21

R2(config-router)#redistribute ospf 20 metric-type 1 subnets route-map OSPF20\_TO\_OSPF21

1. **无线网络基础部署**

* 分公司使用EG1作为无线用户和无线FIT AP的DHCP 服务器；

service dhcp

ip dhcp excluded-address 192.1.50.252 192.1.50.254

ip dhcp excluded-address 192.1.60.252 192.1.60.254

!

ip dhcp pool AP

option 138 ip 10.2.0.12

network 192.1.50.0 255.255.255.0

default-router 192.1.50.254

!

ip dhcp pool yonghu

network 192.1.60.0 255.255.255.0

default-router 192.1.60.254

* 创建分公司内网 SSID 为 Ruijie\_Fit\_XX(XX现场提供)，WLAN ID 为1，AP-Group为Ruijie，内网无线用户关联SSID后可自动获取VLAN60地址。
* 为降低AC性能压力，Fit AP统一采用本地转发模式；

FW-WS6008-VAC(config)#wlan-config 1 Ruijie\_Fit\_1

FW-WS6008-VAC(config-wlan)#TUnnel LOcal

FW-WS6008-VAC(config-wlan)#exi

FW-WS6008-VAC(config)#ap-group Ruijie

FW-WS6008-VAC(config-group)#interface-mapping 1 60 ap-wlan-id 1

FW-WS6008-VAC(config-group)#tunnel local wlan 1 vlan 60

FW-WS6008-VAC(config-group)#exi

1. **无线安全部署**

* 连接Fit AP的无线用户接入无线网络时采用WPA2加密方式，加密密码为XX(现场提供)；

FW-WS6008-VAC(config)#wlansec 1

FW-WS6008-VAC(config-wlansec)#security rsn enable

FW-WS6008-VAC(config-wlansec)#security rsn ciphers aes enable

FW-WS6008-VAC(config-wlansec)#security rsn akm psk enable

FW-WS6008-VAC(config-wlansec)#security rsn akm psk set-key ascii 12345678

* 限制AP的每个射频卡最大带点人数为16人；
* 调整2.4G频段射频卡powerlocal功率数值为20，5.8G频段射频卡powerlocal功率数值为100，尽量降低同频干扰带来的影响；
* 调整5.8G射频卡无线频率带宽至40MHz，增大数据传输带宽；
* 为保证终端走到AP覆盖的边缘区域，终端能够及时发起漫游，调整Coverage-area-control功率参数：5.8G 的Coverage-area-control功率调整为17db, 2.4G 的Coverage-area-control功率调整为10db；

FW-WS6008-VAC(config)#ap-config 5869.6cac.fd4f

You are going to config AP(5869.6cac.fd4f), which is online now.

FW-WS6008-VAC(config-ap)#ap-name FZ1-AP520-AP2

The AP(FZ1-AP520-AP2) is on line.

FW-WS6008-VAC(config-ap)#ap-group Ruijie

FW-WS6008-VAC(config-ap)#sta-limit 16 radio 1

FW-WS6008-VAC(config-ap)#sta-limit 16 radio 2

FW-WS6008-VAC(config-ap)#power local 20 radio 1

FW-WS6008-VAC(config-ap)#power local 100 radio 2

FW-WS6008-VAC(config-ap)#coverage-area-control 10 radio 1

FW-WS6008-VAC(config-ap)#coverage-area-control 17 radio 2

FW-WS6008-VAC(config-ap)#chan-width 40 radio 2

FW-WS6008-VAC(config-ap)#ap-config 5869.6cd6.8fc5

You are going to config AP(5869.6cd6.8fc5), which is online now.

FW-WS6008-VAC(config-ap)#ap-name FZ1-AP520-01

The AP(FZ1-AP520-01) is on line.

FW-WS6008-VAC(config-ap)#ap-name FZ1-AP520-AP1

The AP(FZ1-AP520-AP1) is on line.

FW-WS6008-VAC(config-ap)#ap-group Ruijie

FW-WS6008-VAC(config-ap)# sta-limit 16 radio 1

FW-WS6008-VAC(config-ap)# sta-limit 16 radio 2

FW-WS6008-VAC(config-ap)# power local 20 radio 1

FW-WS6008-VAC(config-ap)# power local 100 radio 2

FW-WS6008-VAC(config-ap)# coverage-area-control 10 radio 1

FW-WS6008-VAC(config-ap)# coverage-area-control 17 radio 2

FW-WS6008-VAC(config-ap)# chan-width 40 radio 2

* 关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

FW-WS6008-VAC(config)#ac-controller

FW-WS6008-VAC(config-ac)#802.11a network rate 6 disabled

FW-WS6008-VAC(config-ac)#802.11a network rate 9 disabled

FW-WS6008-VAC(config-ac)#802.11b network rate 1 disabled

FW-WS6008-VAC(config-ac)#802.11b network rate 2 disabled

FW-WS6008-VAC(config-ac)#802.11b network rate 5 disabled

FW-WS6008-VAC(config-ac)#802.11g network rate 5 disabled

FW-WS6008-VAC(config-ac)#802.11g network rate 2 disabled

FW-WS6008-VAC(config-ac)#802.11g network rate 1 disabled

出口NAT部署

具体配置参数如下：

 出口网关上进行NAT配置实现机构内网终端及服务器均可访问互联网，通过NAPT方式将内网IP地址转换到互联网接口上；

EG1:

FZ1-EG2000-EG1(config)#ip nat pool nat\_pool prefix-length 24

FZ1-EG2000-EG1(config-ipnat-pool)# address interface GigabitEthernet 0/4 match interface GigabitEthernet 0/4

FZ1-EG2000-EG1(config)# ip nat inside source list 110 pool nat\_pool overload

FZ1-EG2000-EG1(config)#ip access-list extended 110

FZ1-EG2000-EG1(config-ext-nacl)# 10 permit ip 192.1.10.0 0.0.0.255 any

FZ1-EG2000-EG1(config-ext-nacl)# 20 permit ip 192.1.20.0 0.0.0.255 any

FZ1-EG2000-EG1(config-ext-nacl)# 30 permit ip 192.1.50.0 0.0.0.255 any

FZ1-EG2000-EG1(config-ext-nacl)# 40 permit ip 192.1.60.0 0.0.0.255 any

FZ1-EG2000-EG1(config-ext-nacl)#int gi0/1

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/1)#ip nat in

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/1)#int gi0/2

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/2)#ip nat in

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/2)#int gi0/4

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/4)#ip nat outside

EG2：

FW-EG2000-EG2(config)#ip access-list ex 110

FW-EG2000-EG2(config-ext-nacl)#permit ip 172.16.0.0 0.0.3.255 any

FW-EG2000-EG2(config-ext-nacl)#exit

FW-EG2000-EG2(config)#ip nat pool nat\_pool prefix-length 24

FW-EG2000-EG2(config-ipnat-pool)# address interface GigabitEthernet 0/4 match interface GigabitEthernet 0/4

FW-EG2000-EG2(config)#int gi0/1

FW-EG2000-EG2(config-if-GigabitEthernet 0/1)#ip nat in

FW-EG2000-EG2(config-if-GigabitEthernet 0/1)#int gi0/4

FW-EG2000-EG2(config-if-GigabitEthernet 0/4)#ip nat out

 出口网关EG1上配置，使交换S1（192.XX.100.1）设备的Telnet服务可以通过互联网被访问，将其地址映射至运营商线路上，映射地址为11.1.2.10，映射端口23333。

EG1：

FZ1-EG2000-EG1(config)# ip nat in source static tcp 192.1.100.1 23 11.1.2.10 23333

Web Portal用户认证部署

 在网关EG1上启用Web Portal认证服务，认证用户名密码均为user1、user2；

 有线用户需进行WEB认证访问互联网；

 无线用户不需在EG上进行WEB认证即可访问互联网。







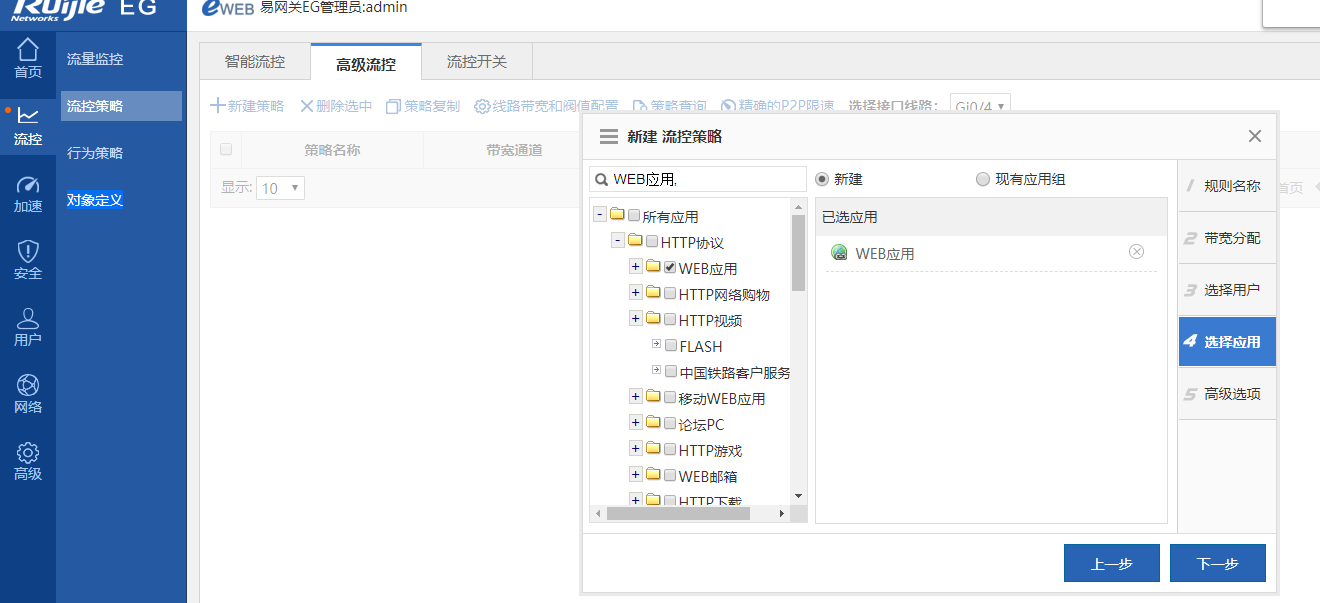
应用流量控制部署

 EG1针对内网访问互联网WEB流量限速每IP 1000Kbps，内网WEB总流量不超过20Mbps，通道名称定义为WEB。











用户行为策略部署

 EG1基于网站访问、邮件收发、IM聊天、论坛发帖、搜索引擎多应用启用审计功能；



 EG1周一到周六工作时间09：00—17:00（命名为work）阻断并审计P2P应用软件使用,审计策略名称定义为P2P。





VPN部署

为了实现总部服务器区与分支机构互访数据的安全性，针对来往数据使用VPN技术进行安全保障，具体规划如下：

 EG1与EG2出口网关间启用GRE Over IPSec VPN嵌套功能；

 GRE隧道内部承载OSPF协议，使其总分机构间内网连通；

 IPSec使用静态点对点模式，esp传输模式封装协议，isakmp策略定义加密算法采用3des，散列算法采用md5，预共享密码为 ruijie，DH使用组2。转换集myset定义加密验证方式为 esp-3des esp-md5-hmac ，感兴趣流ACL编号为103,加密图定义为mymap;

EG1:

FZ1-EG2000-EG1(config)#ip access-list ex 103

FZ1-EG2000-EG1(config-ext-nacl)#permit ip 11.1.2.10 0.0.0.0 11.1.1.10 0.0.0.0

FZ1-EG2000-EG1(config-ext-nacl)#exit

FZ1-EG2000-EG1(config)#crypto isakmp key 0 ruijie address 11.1.1.10

FZ1-EG2000-EG1(config)#crypto isakmp policy 1

FZ1-EG2000-EG1(isakmp-policy)#au pre-share

FZ1-EG2000-EG1(isakmp-policy)#ha md5

FZ1-EG2000-EG1(isakmp-policy)#encryption 3des

FZ1-EG2000-EG1(isakmp-policy)#group 2

FZ1-EG2000-EG1(isakmp-policy)#exit

FZ1-EG2000-EG1(config)#crypto ipsec transform-set myset esp-3des esp-md5-hmac

FZ1-EG2000-EG1(cfg-crypto-trans)#exit

FZ1-EG2000-EG1(config)#crypto map mymap 10 ipsec-isakmp

FZ1-EG2000-EG1(config-crypto-map)#match address 103

FZ1-EG2000-EG1(config-crypto-map)#set transform-set myset

FZ1-EG2000-EG1(config-crypto-map)#set peer 11.1.1.10

FZ1-EG2000-EG1(config-crypto-map)#int gi0/4

FZ1-EG2000-EG1(config-if-GigabitEthernet 0/4)#crypto map mymap

EG1(config)#int tunn 0

EG1(config-if-Tunnel 0)#tun source 11.1.2.10

EG1(config-if-Tunnel 0)#tun destination 11.1.1.10

EG1(config-if-Tunnel 0)#ip address 11.1.5.2 30

EG1(config-if-Tunnel 0)#rou ospf 30

EG1(config-router)#network 11.1.5.2 0.0.0.3 a 0

EG2:

FW-EG2000-EG2(config)#ip access-list ex 103

FW-EG2000-EG2(config-ext-nacl)#permit ip 11.1.1.10 0.0.0.0 11.1.2.10 0.0.0.0

FW-EG2000-EG2(config-ext-nacl)#crypto isakmp key 0 ruijie address 11.1.2.10

FW-EG2000-EG2(config)#crypto isakmp policy 1

FW-EG2000-EG2(isakmp-policy)#au pre-share

FW-EG2000-EG2(isakmp-policy)#ha md5

FW-EG2000-EG2(isakmp-policy)#encryption 3des

FW-EG2000-EG2(isakmp-policy)#group 2

FW-EG2000-EG2(isakmp-policy)# crypto ipsec transform-set myset esp-3des esp-md5-hmac

FW-EG2000-EG2(cfg-crypto-trans)#exit

FW-EG2000-EG2(config)#crypto map mymap 10 ipsec-isakmp

FW-EG2000-EG2(config-crypto-map)#match address 103

FW-EG2000-EG2(config-crypto-map)#set transform-set myset

FW-EG2000-EG2(config-crypto-map)#set peer 11.1.2.10

FW-EG2000-EG2(config-crypto-map)#int gi0/4

FW-EG2000-EG2(config-if-GigabitEthernet 0/4)#crypto map mymap

EG2(config)#int tunn 0

EG2(config-if-Tunnel 0)#tun sou 11.1.1.10

EG2(config-if-Tunnel 0)#tun des 11.1.2.10

EG2(config-if-Tunnel 0)#ip ad 11.1.5.1 30

EG2(config-if-Tunnel 0)#rou ospf 10

EG2(config-router)#network 11.1.5.0 0.0.0.3 a 0

 各办事处通过PC桌面SSLVPN客户端访问总部服务器区发布资源，访问地址为https://11.1.1.10,拨入客户端获取地址为10.10.10.0/24，DNS为8.8.8.8，隧道资源名称为Server包含172.16.0.0/22与10.2.0.12，登录用户名密码均为user1、user2。







