任务 2：网络安全设备配置与防护（240 分）

1. 总部核心交换机 DCRS 上开启 SSH 远程管理功能，本地认证用户名:2019DCN,密码: DCN2019;（6 分）

```
username 2019DCN privilege 15 password 0 DCN2019
!
```

设置正确用户名和密码匹配题目要求 3 分，错配少配不得分;

```
ssh-server enable
```

全局启用 SSH 服务 3 分，错配少配不得分;

2. 总部启用 MSTP 协议，NAME 为 2019DCN、 Revision-level 1，实例 1 中包括 VLAN10；实例 2 中包括 VLAN20、要求两条链路负载分担,其中 VLAN10 业务数据在 E1/0/4 进行数据转发，要求 VLAN20 业务数据在 E1/0/5 进行数据转发,通过在 DCWS 两个端口设置 COST 值 2000000 实现;配置 DCRS 连接终端接口立即进入转发模式且在收到 BPDU 时自动关闭端口;防止从 DCWS 方向的根桥抢占攻击;（6 分）

DCRS:

```
spanning-tree mst configuration
 name 2019DCN
 revision-level 1
 instance 0 vlan 1-9;11-19;21-4094
 instance 1 vlan 10
 instance 2 vlan 20
 exit
```

spanning-tree

spanning-tree mst 1 priority 0

spanning-tree mst 2 priority 0

1.DCRS 上实例 1 关联 VLAN 10 、实例 2 关联 VLAN 20 NAME ： 2019DN 共 1 分,错配少配不得分;

DCWS:

panning-tree mst configuration

name 2019DCN

revision-level 1

instance 0 vlan 1-9;11-19;21-4094

instance 1 vlan 10

instance 2 vlan 20

2.DCWS 上实例 1 关联 VLAN 10 、实例 2 关联 VLAN 20 NAME ： 2019DN 共 1 分 ， 错配少配不得分;

Interface Ethernet1/0/4

spanning-tree mst 2 cost 2000000

Interface Ethernet1/0/5

spanning-tree mst 1 cost 2000000

3.在 DCWS 端口 E1/0/4-E1/0/5 配置正确 1 分, 错配少配不得分;

Interface Ethernet1/0/7-12

spanning-tree portfast bpduguard

4.在 DCRS 上 E1/0/7-E1/0/12 配置共 1 分 . 错配少配不得分;

Interface Ethernet1/0/7

spanning-tree mst 1 rootguard

Interface Ethernet1/0/8

spanning-tree mst 2 rootguard

Interface Ethernet1/0/9

spanning-tree mst 1 rootguard

Interface Ethernet1/0/10

spanning-tree mst 2 rootguard

Interface Ethernet1/0/11

spanning-tree mst 2 rootguard

Interface Ethernet1/0/12

spanning-tree mst 2 rootguard

5.在 DCRS 端口 E1/0/4 /E1/0/5 根桥保护配置正确共 2 分,错配少配每处扣 1 分，扣完为止;

3. 尽可能加大总部核心交换机 DCRS 与防火墙 DCFW 之间的带宽，模式为动态方式; (6 分)

Interface Ethernet1/0/1

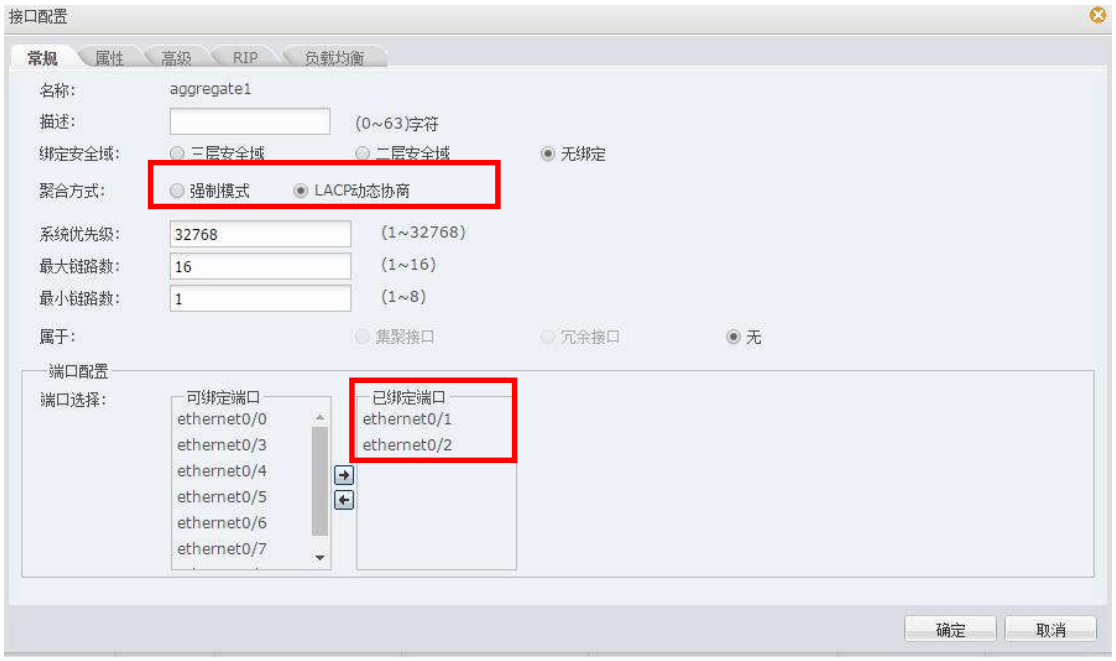
switchport mode trunk

port-group 1 mode active

Interface Ethernet1/0/2

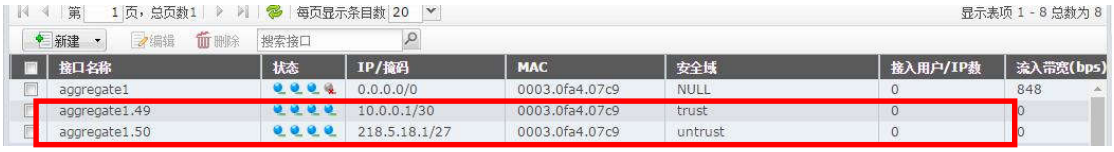
switchport mode trunk

port-group 1 mode active



1.DCRS E1/0/1,E1/0/2 口下配置 TRUNK2 分和 LACP 1 分，创建 aggreate1 接口模式 2 分选择 LACP 动态协商 1 分,共 6 分,错配少配不得分;

4. 配置使总部 VLAN10，30，40 业务的用户访问 INTERNET 往返数据流都经过 DCFW 进行最严格的安全防护;(6 分)



1.创建 aggreate1.49 接口 1 分，aggreate1.50 接口 1 分;

2.策略放行 1 分，错配少配不得分;

3.静态路由 1 分，错配少配不得分;

状态	IP/掩码	下一跳	下一跳接口	协议	优先权	度量	路由权值	track状态	描述
	0.0.0.0/0	218.5.18.2		静态	1	0	1		
	172.16.10.0/24	10.0.0.2		静态	1	0	1		
	172.16.30.0/24	10.0.0.2		静态	1	0	1		
	172.16.40.0/24	10.0.0.2		静态	1	0	1		
	192.168.1.0/24		ethernet0/0	直连	0	0	1		
	192.168.1.1/32		ethernet0/0	主机	0	0	1		

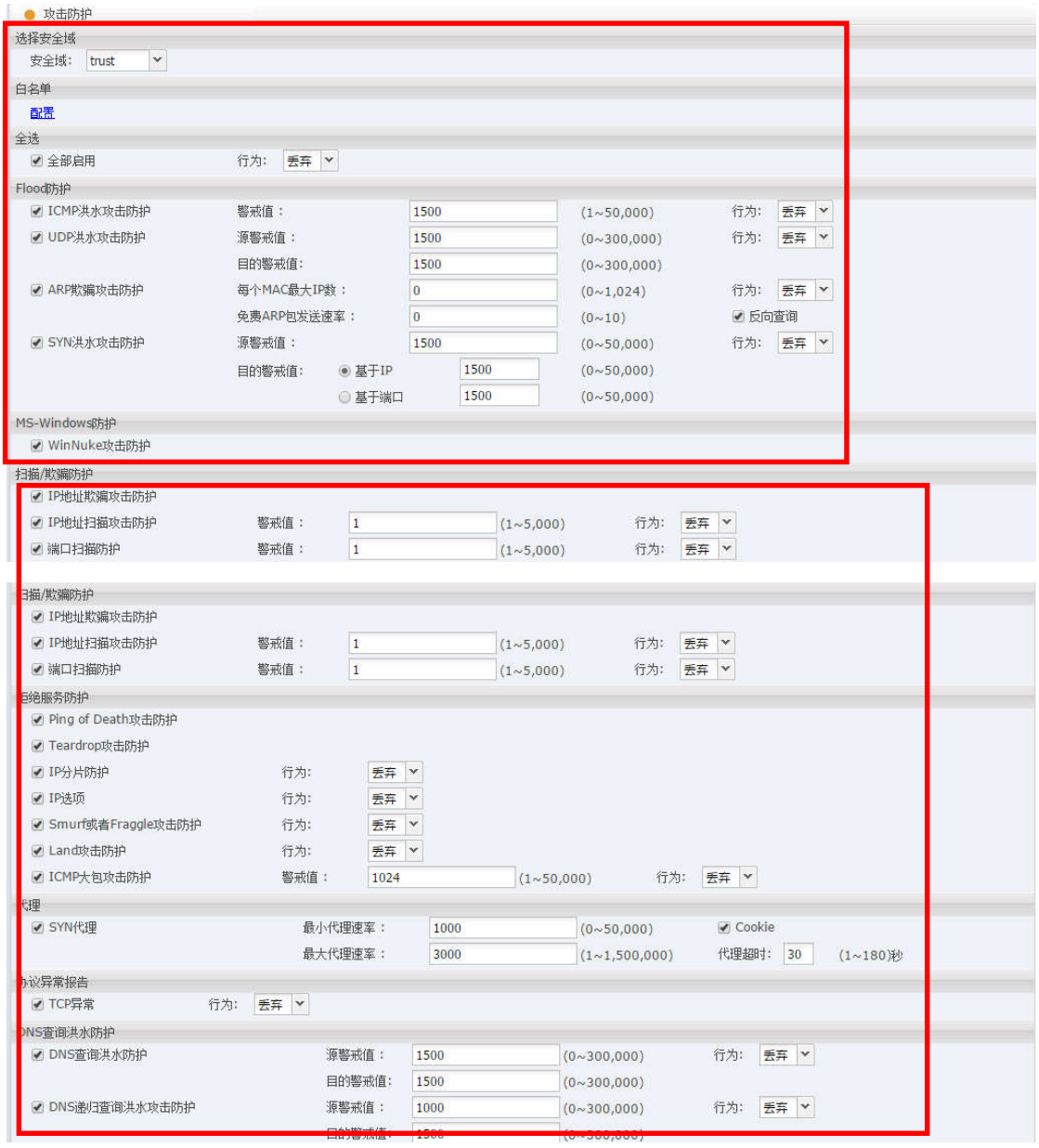
```
ip access-list extended yewu
  permit ip 172.16.10.0 0.0.0.255 any-destination
  permit ip 172.16.30.0 0.0.0.63 any-destination
  permit ip 192.168.40.0 0.0.0.255 any-destination
```

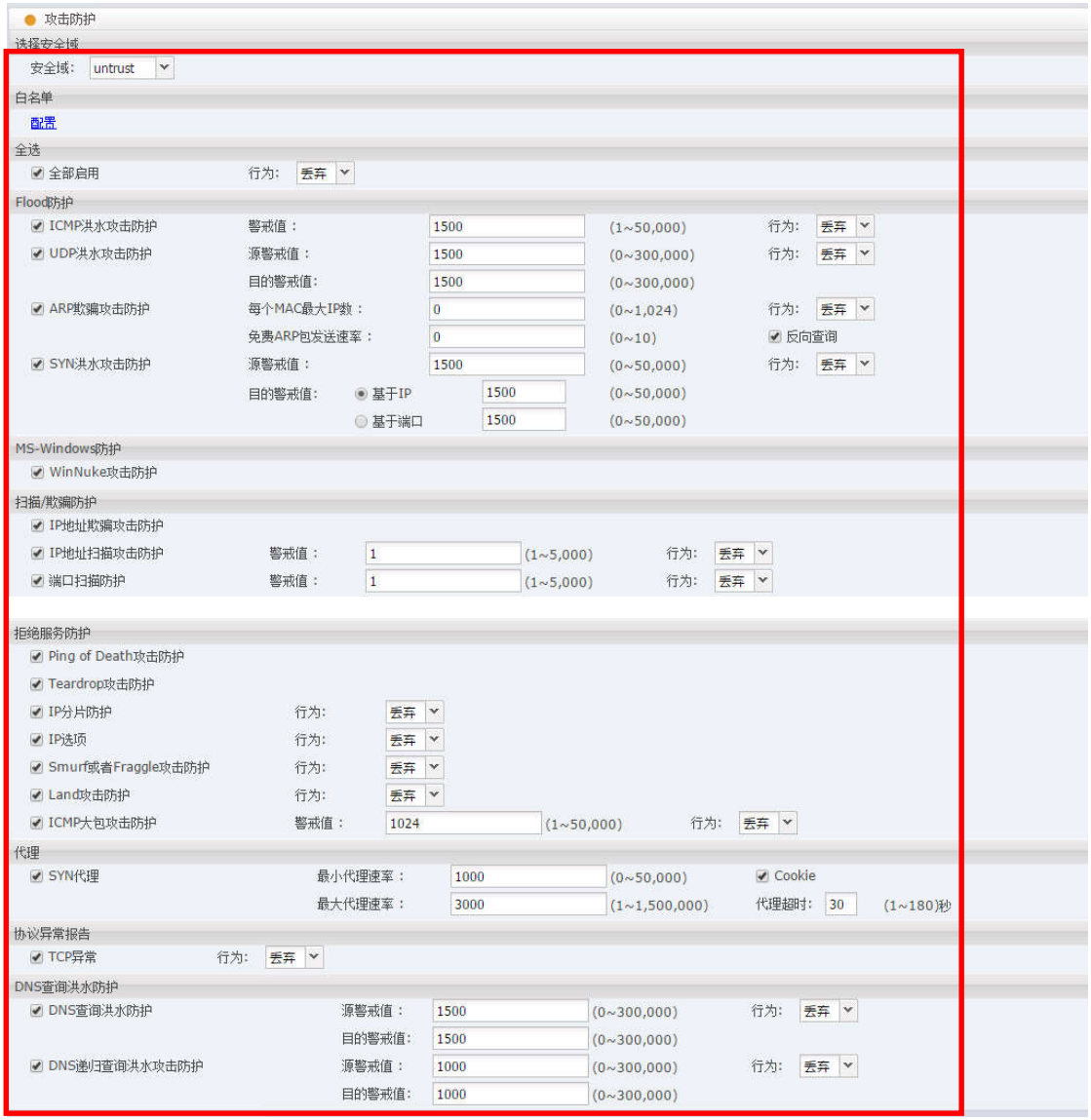
```
ip access-list extended hui
  permit ip any-source host-destination 218.5.18.9
  permit ip any-source host-destination 218.5.18.10
  exit
```

```
class-map hui
 match access-group hui
class-map yewu
 match access-group yewu
policy-map yewu
 class yewu
 set ip nexthop  218.5.18.1
 exit
policy-map hui
 class hui
```

```
set ip nexthop  10.0.0.1
Interface Ethernet1/0/7-12, 1/0/4-5
 service-policy input yewu
Interface Ethernet1/0/24
  service-policy input hui
```

4.DCRS 上 PBR，ACL，nethop,接口调用需要完全匹配得 1 分，错配少配不得分，class map 可自行定义；





5.DCFW TRUST,UNTRUST 上开启所有攻击防护得 1 分，错配少配不得分;

5. 总部核心交换机 DCRS 上实现 VLAN40 业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后该端口，恢复时间为 30 分钟；（6 分）

!

```
vlan 40
isolate-port apply 12
```

1.错配少配不得分，2 分;

```
loopback-detection interval-time 10 10
loopback-detection control-recovery timeout 1800
```

2.全局开启单端口环路检查功能，错配少配不得分； 2 分

```
Interface Ethernet1/0/10-12
loopback-detection specified-vlan 40
 loopback-detection control shutdown
```

3.E1/0/10 到 E1/0/12 口全部配置正确 2 分，错配少配不得分;

6. 总部核心交换机 DCRS 检测到 VLAN40 中私设 DHCP 服务器关闭该端口;（6 分）

```
ip dhcp snooping enable
```

1.全局开启 dhcp snooping 功能 1 分

```
Interface Ethernet1/0/10
 service-policy input yewu
 spanning-tree portfast bpduguard
 switchport access vlan 40
 loopback-detection specified-vlan 40
 loopback-detection control shutdown
 ip dhcp snooping binding user-control
 ip dhcp snooping action shutdown 1 分
Interface Ethernet1/0/11
 service-policy input yewu
 spanning-tree portfast bpduguard
 switchport access vlan 40
```

loopback-detection specified-vlan 40

loopback-detection control shutdown

ip dhcp snooping binding user-control

ip dhcp snooping action shutdown 1 分

!

Interface Ethernet1/0/12

service-policy input yewu

spanning-tree portfast bpduguard

switchport access vlan 40

loopback-detection specified-vlan 40

loopback-detection control shutdown

ip dhcp snooping binding user-control

ip dhcp snooping action shutdown 1 分

Interface Ethernet1/0/4

ip dhcp snooping trust 1 分

Interface Ethernet1/0/5

ip dhcp snooping trust 1 分

2.E1/0/10-E1/0/12 设置 shutdown 共 3 分，错配少配不得分； ；

3.E1/0/4-5 设置 Trust，错配少配不得分； 共 2 分;

7. 总部核心交换机 DCRS 开启某项功能,防止 VLAN40 下 ARP 欺骗攻击;(6 分)

ip dhcp snooping enable

ip dhcp snooping binding enable 3 分

1.全局开启 dhcp snooping binding 功能 3 分

```
Interface Ethernet1/0/10
 service-policy input yewu
 spanning-tree portfast bpduguard
 switchport access vlan 40
 loopback-detection specified-vlan 40
 loopback-detection control shutdown
 ip dhcp snooping binding user-control
 ip dhcp snooping action shutdown
!
Interface Ethernet1/0/11
 service-policy input yewu
 spanning-tree portfast bpduguard
 switchport access vlan 40
 loopback-detection specified-vlan 40
 loopback-detection control shutdown
 ip dhcp snooping binding user-control
 ip dhcp snooping action shutdown
!
Interface Ethernet1/0/12
 service-policy input yewu
 spanning-tree portfast bpduguard
 switchport access vlan 40
 loopback-detection specified-vlan 40
 loopback-detection control shutdown
```

1分

1分

ip dhcp snooping binding user-control 1 分

ip dhcp snooping action shutdown

2.E1/0/10-E1/0/12 接口下设置 binding user-control 共 3 分，错配少配不得分;

8. 总部核心交换机 DCRS 上实现访问控制，在 E1/0/14 端口上配置 MAC 地址为 00-03-0f-00-00-01 的主机不能访问 MAC 地址为 00-00-00-00-00-ff 的主机;（6 分）

mac-access-list extended macACL

deny host-source-mac 00-03-0f-00-00-01 host-destination-mac 00-00-00-00-00-ff

1.全局配置 MAC 扩展 ACL 4 分,错配少配每处 2 分;

Interface Ethernet1/0/14

mac access-group macACL in

2.接口应用访问控制列表 2 分，调用错误都不得分（ACL 名字可自定义但不能调用错误）;

9. 2017 年勒索蠕虫病毒席卷全球，爆发了堪称史上最大规模的网络攻击，通过对总部核心交换机 DCRS 所有业务 VLAN 下配置访问控制策略实现双向安全防护;（6 分）!

ip access-list extended bingdu

deny tcp any-source any-destination d-port 135

deny tcp any-source any-destination d-port 137

deny tcp any-source any-destination d-port 138

deny tcp any-source any-destination d-port 139

```
deny tcp any-source any-destination d-port 445
permit ip any-source any-destination
```

1.拒绝任何源到任何目的访问 135、137、138、139、445 端口共 4 分，错配少配扣 1 分扣完为止;

```
vacl ip access-group bingdu in vlan 10;20;30;40
vacl ip access-group bingdu out vlan 10;20;30;40
```

2.VACL 调用共 2 分，每处 1 分，错配少配不得分;

10.总部部署了一套网管系统实现对 DCRS 交换机进行管理，网管系统 IP 为：172.16.100.21，读团体值为：DCN2019，版本为 V2C，交换机 DCRS Trap 信息实时上报网管，当 MAC 地址发生变化时，也要立即通知网管发生的变化，每 35s 发送一次；（6 分）

```
snmp-server enable
```
1 分

```
snmp-server host 172.16.100.21 v2c DCN2019
```
1 分

```
snmp-server enable traps
```
1 分

```
snmp-server enable traps mac-notification
```
1 分

```
mac-address-table notification
```
1 分

```
mac-address-table notification interval 35
```
1 分

共 6 分，错配少配不得分;

11.总部核心交换机 DCRS 出口往返流量发送给 DCBI，由 DCBI 对收到的数据进行用户所要求的分析；（6 分）

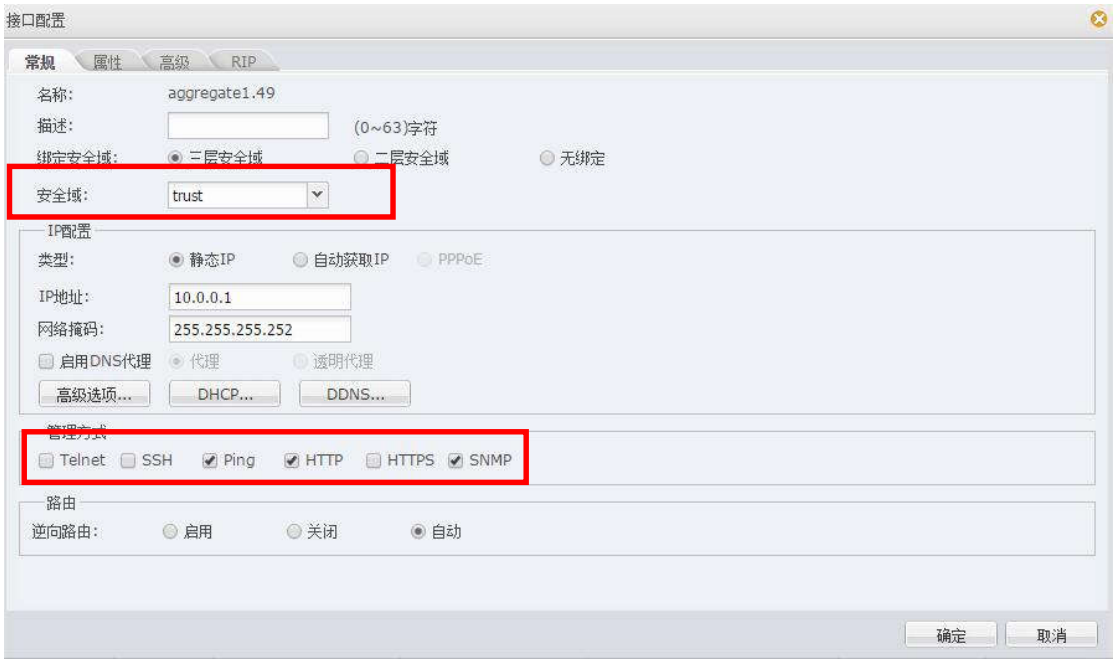
```
monitor session 1 source interface Ethernet1/0/24 tx
monitor session 1 source interface Ethernet1/0/24 rx
```

1.源镜像端口 E1/0/24 口，错配少配不得分； 3 分

```
monitor session 1 destination interface Ethernet1/0/3
```

2.目的镜像端口 E1/0/3 口，错配少配不得分； 3 分

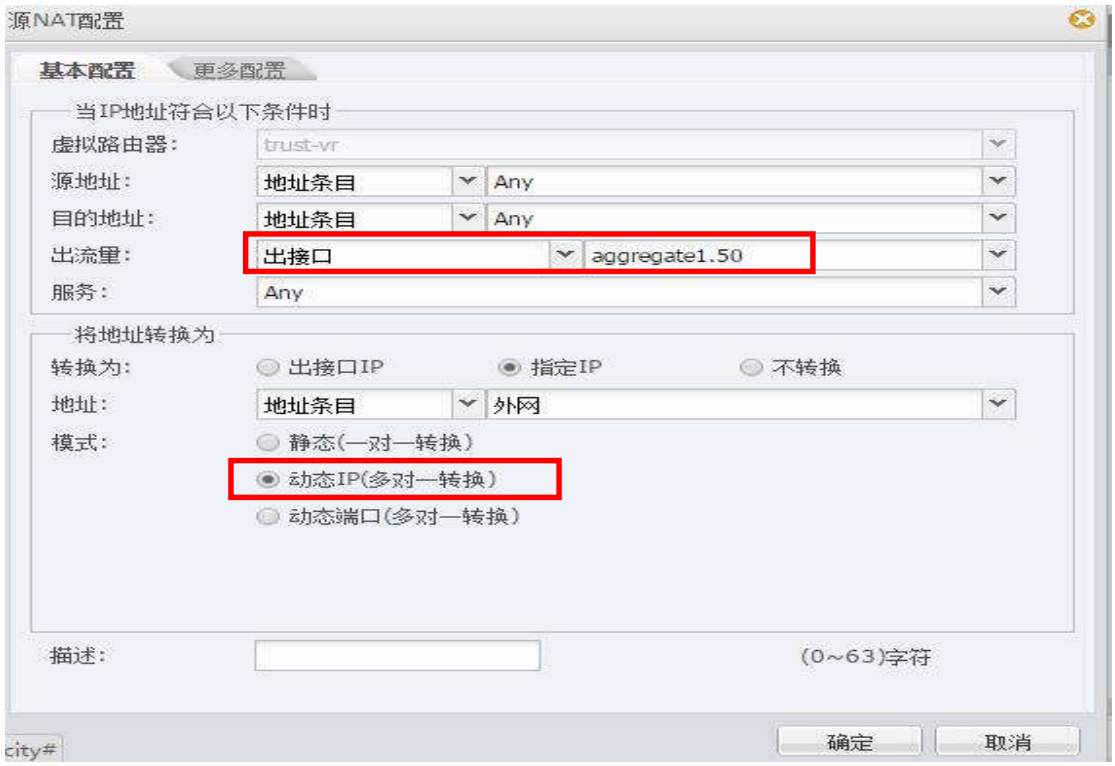
12.为实现对防火墙的安全管理，在防火墙 DCFW 的 Trust 安全域开启 PING,HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能；(6 分)



1.Trust 安全域、开启：PING、 HTTP、 SNMP 功能共 3 分。错配少配不得分。

2. Untrust 安全域、开启：SSH、 HTTPS 功能 共 3 分，错配少配不得分。

13. 总部 VLAN 业务用户通过防火墙访问 Internet 时，轮询复用公网 IP： 218.5.18.9、218.5.18.10； （6 分）



1.创建公网 ip 地址对象，错配少配不得分；2 分

2.创建源 NAT 出接口 aggreate1.50 模式：动态 IP，错配少配不得分；4 分

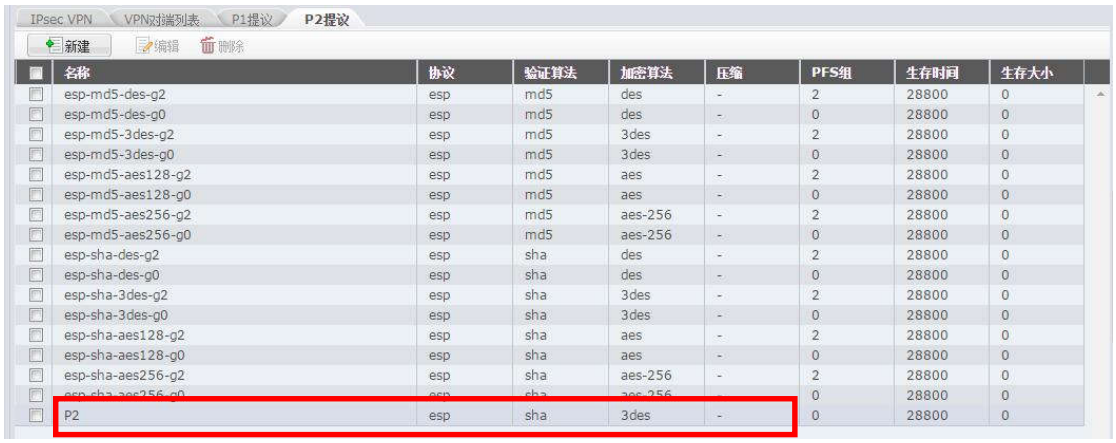
14.项目二期要启用云端路由器，需要在总部防火墙DCFW上完成以下预配:

防火墙DCFW与云端路由器220.5.22.3建立GRE隧道，并使用IPSec保护GRE隧道，保证隧道两端2.2.2.2与VLAN20安全通信。

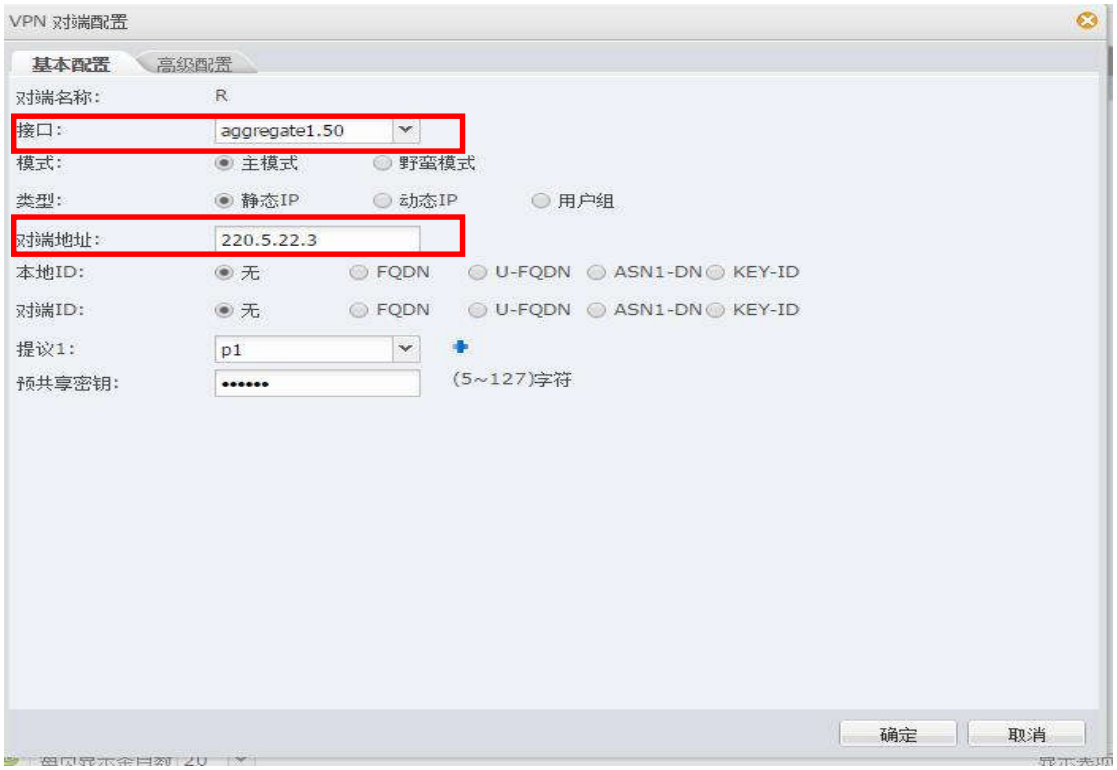
第一阶段　采用pre-share认证 加密算法:3DES;

第二阶段　采用ESP协议，　加密算法:3DES，预设共享秘钥:DCN2019（6分）

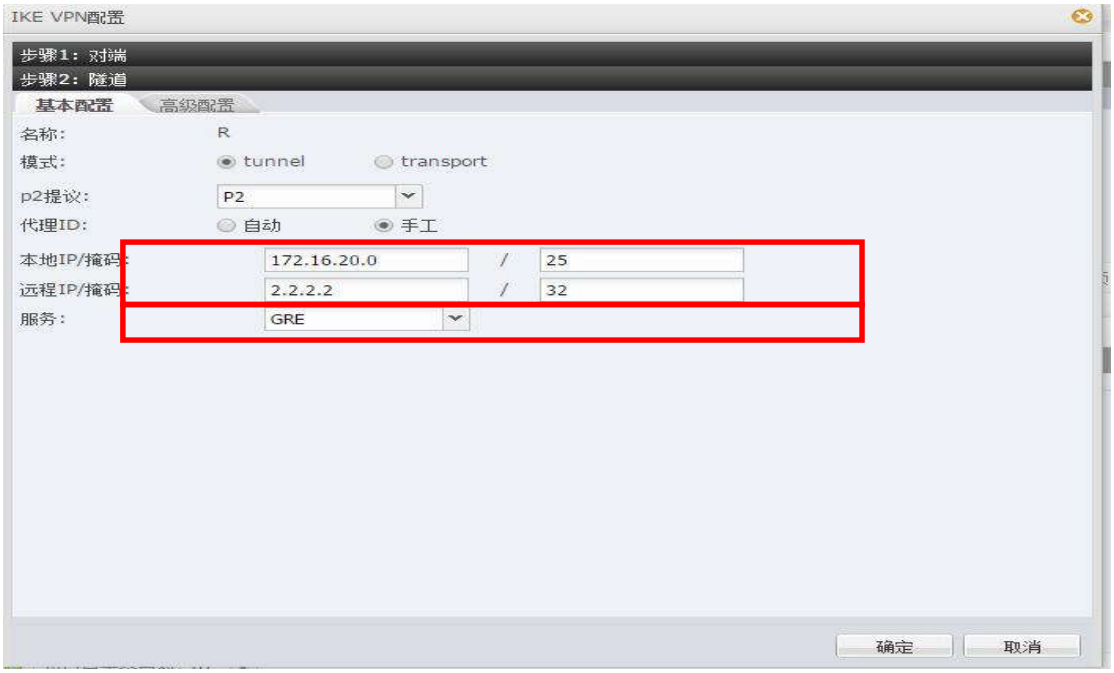
WEB界面配置答案



1.按要求创建提议1和提议2共1分，错配少配不得分；



2.绑定防火墙aggregate1.50 设置对端IP匹配题目地址2 分，错配少配不得分；此处配置错误本次后面不得分；



3.设置本地VLAN 20网段和远程网段绑定GRE服务2分，错配少配不得分；

	ID	名称	状态	有效性	源安全域	目的安全域	源地址	目的地址	角色/用户/用户组	服务
	1			是	VPNHub	trust	Any(地址条目)	Any(地址条目)		Any
	2			是	trust	VPNHub	Any(地址条目)	Any(地址条目)		Any

4.VPNHub与Trust策略双向放行1分，错配少配不得分；

15.配置RIP完成云端路由器2.2.2.2、DCFW、总部核心交换机VLAN20的连通性，使用MD5认证，密钥为DCN2019；（6分）

DCFW:

```
ip vrouter "trust-vr"
router  rip
network  12.12.12.0/24
network  172.16.200.0/24
```

1分

```
interface aggregate1.200
ip rip authentication mode md5
```

2分

```
ip rip authentication string DCN2019
```
（密码会被加密，可以不一致）

1分

DCRS:

```
router rip
version 2
network 172.16.20.0/24
network 172.16.200.0/24
```
1分

```
address-family ipv4 vrf 1
interface Vlan200
 ip rip authentication mode md5
 ip rip authentication string DCN2019
```
1分

共6分，某项错配少配不得分；（FW认证密钥会加密，可以不一致）

16.总部核心交换机 DCRS 上使用某种技术，将 VLAN20 通过 RIP 连接云端路由器路由与本地其它用户访问 INTERNET 路由隔离;（6 分）

```
ip vrf 1
```
（1 分）

```
interface Vlan20
ip vrf forwarding 1
```
（1 分）

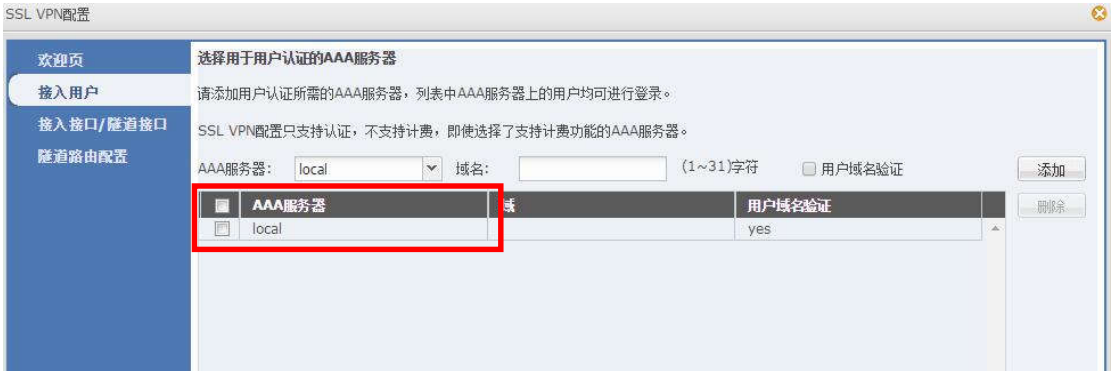
```
interface Vlan200
ip vrf forwarding 1
```
（1 分）

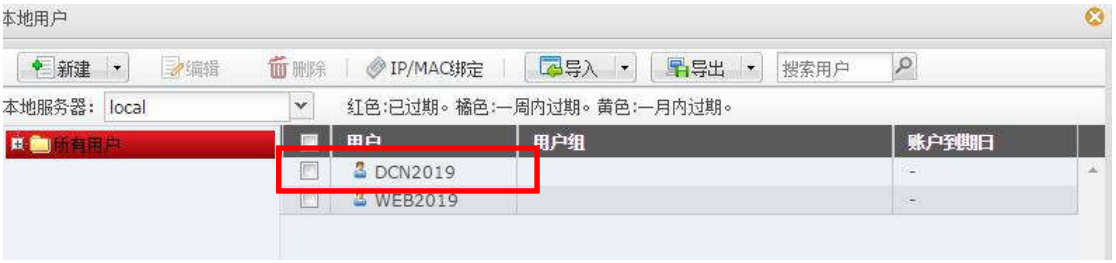
```
router rip
address-family ipv4 vrf 1
```
3 分

共 6 分，某项错配少配该项不得分。（VRF 名称可以自定义，调

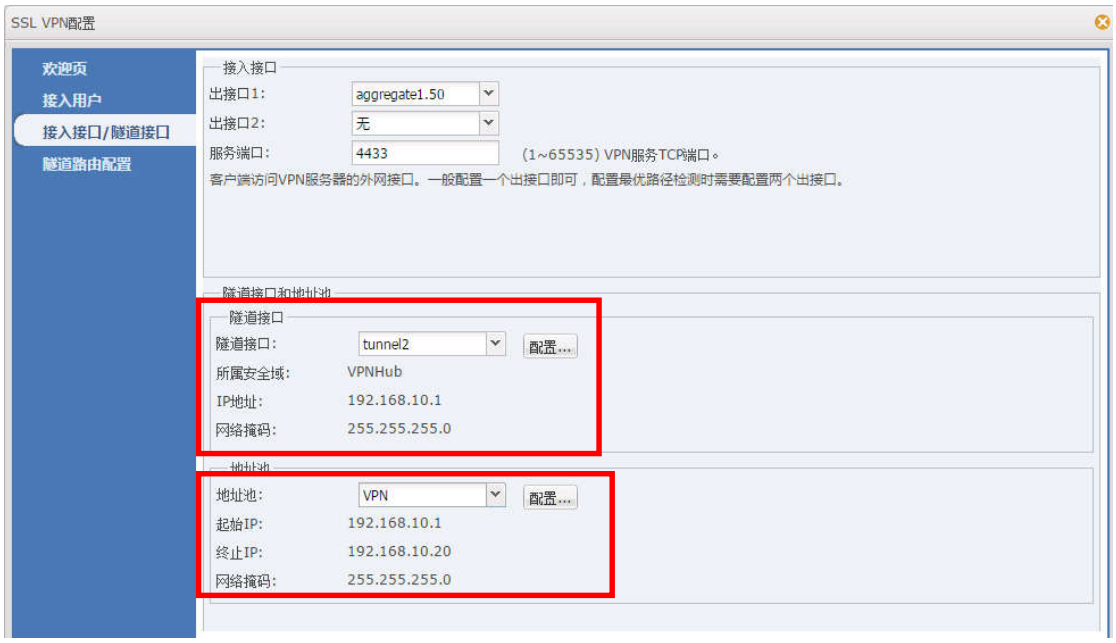
用正确即可，可以不一致）

17. 远程移动办公用户通过专线方式接入总部网络，在防火墙 DCFW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 DCN2019，地址池参见地址表；（6 分）





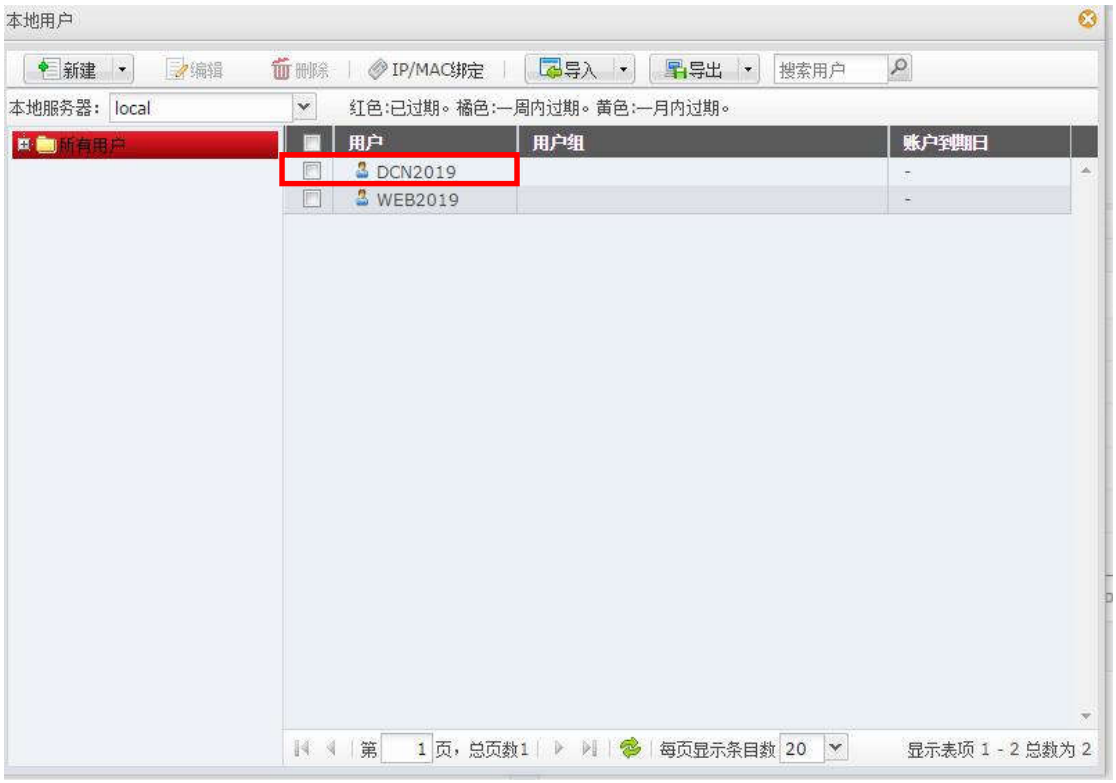
1. 设置认证服务器和认证账号 2 分，错配少配不得分；



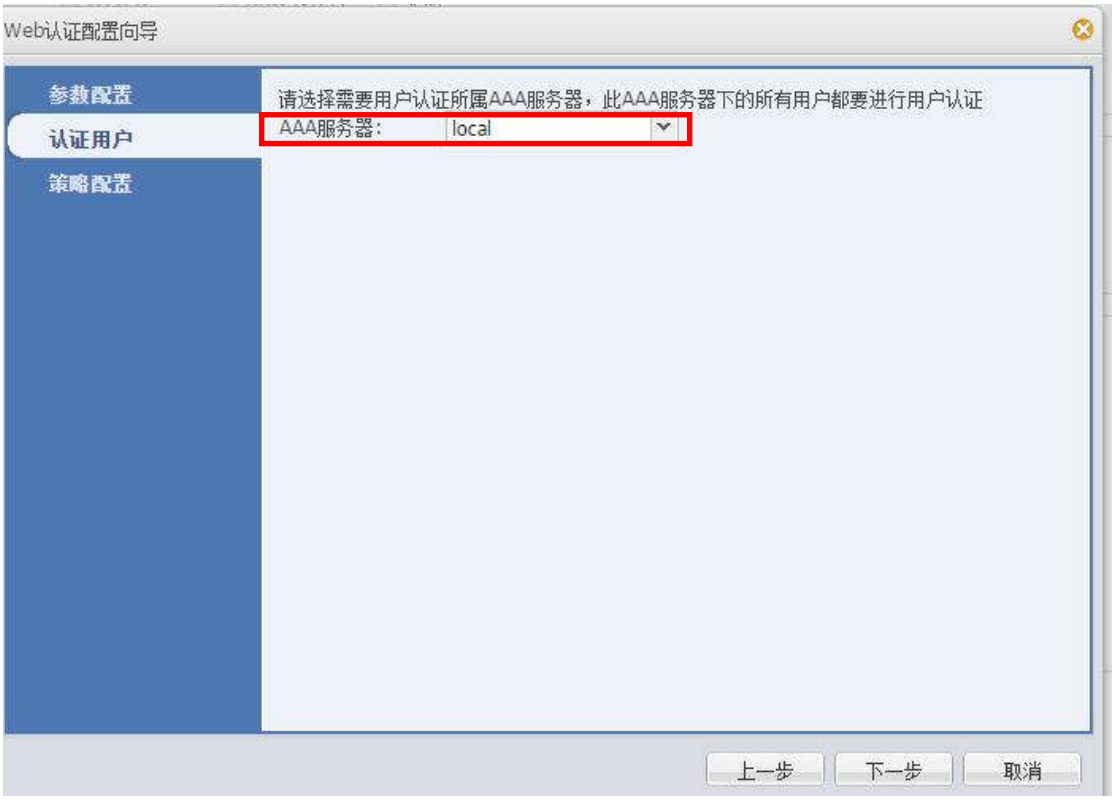
2.创建地址池和隧道接口匹配 IP 地址表共 2 分，错配少配不得分；

3.创建安全策略 Untrust 目的地址 VLAN 30 网段 2 分，错配少配不得分；

18.出于安全考虑，无线用户移动性较强，无线用户访问 INTERNET 时需要采用认证，在防火墙上开启 WEB 认证，账号密码为 DCN2019；（6 分）

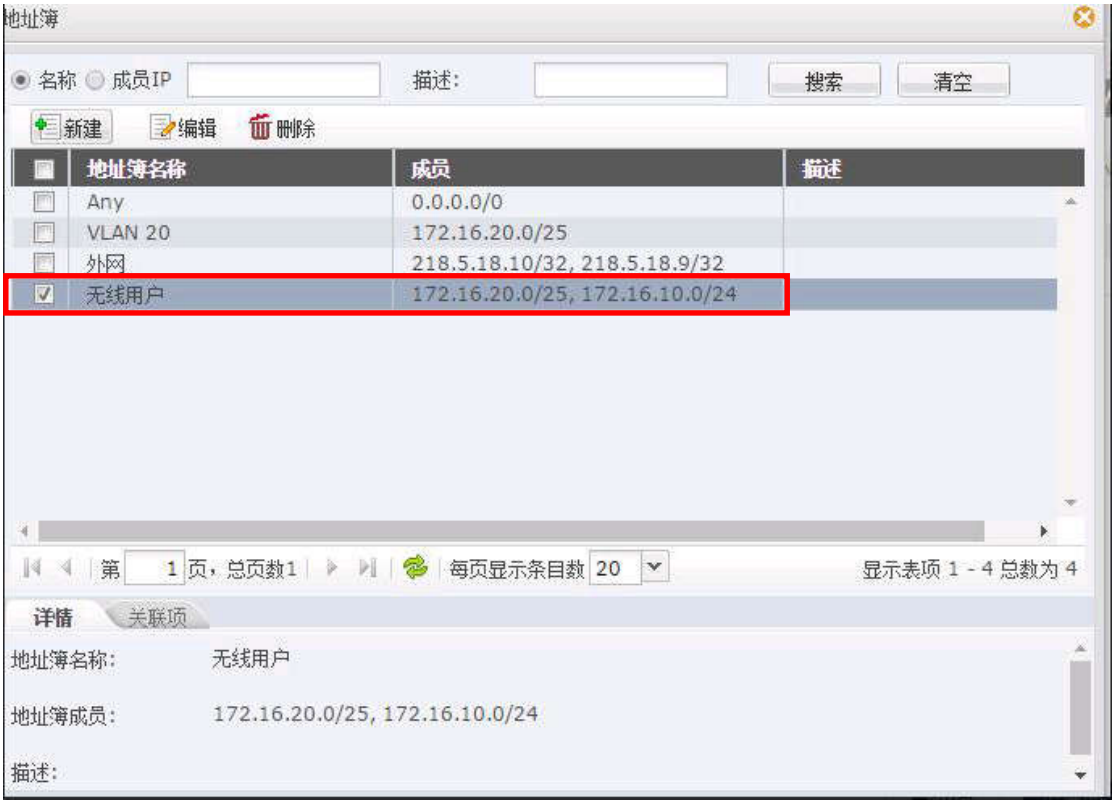


1.添加认证账号 1 分，错配少配不得分;



2. 添加认证服务器 1 分，错配少配不得分；

3. 设置 WEB 认证参数 1 分，错配少配不得分；



4. 无线用户地址簿 1 分，错配少配不得分；

5. 设置安全策略共 2 分缺，错配或少配扣 1 分，扣完为止；

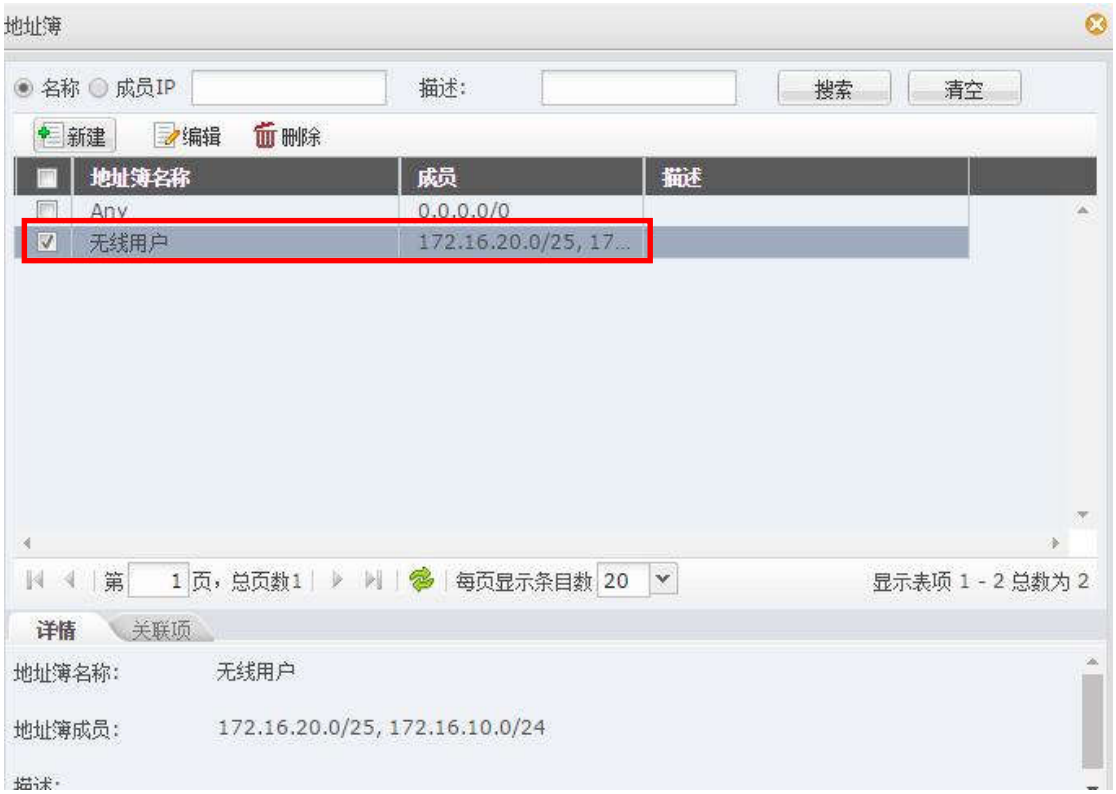
19. 为了保证带宽的合理使用，通过流量管理功能将引流组的应用数据流，上行带宽设置为 2M，下行带宽设置为 4M;（6 分）

1. 绑定 Untrust 区域接口，错配少配不得分；2 分

2. 匹配应用：引流组，错配少配不得分； 2 分

3.带宽设置对应题目数值，错配少配不得分； 2分

20.为净化上网环境，要求在防火墙DCFW做相关配置，禁止无线用户周一至周五工作时间9：00-18：00的邮件内容中含有“病毒”、“赌博”的内容，且记录日志；（6分）



1.创建用户对象：1分，错配少配不得分；

2

2.创建时间对象：1分，错配少配不得分；

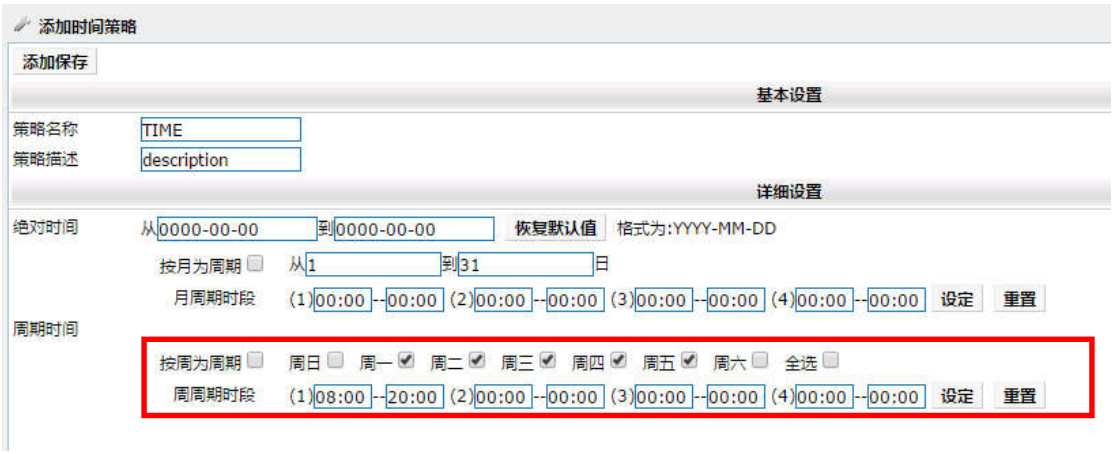
3.创建关键字符合题目参数，行为：记录日志 1分，错配少配不得分；

4.绑定安全域、 时间对象 、用户对象、勾选邮件内容共3分，每处错配少配扣1分，扣完为止；

21. DCBI 配置应用及应用组“流媒体”，UDP 协议端口号范围 10867-10868，在周一至周五 8：00-20：00 监控内网中所有用户的“流媒体”访问记录（6 分）

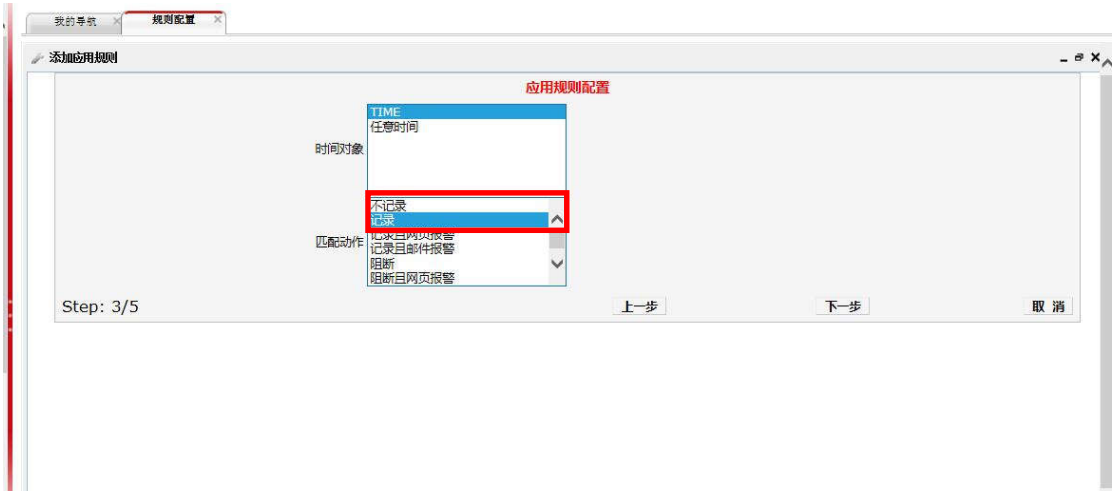
端口号以实际题目中参数为准

1. 创建自定义应用匹配题目参数：1 分，错配少配不得分；



2. 创建时间对象匹配题目要求 1 分，错配少配不得分；

3. 添加自定义应用参数 2 分，错配少配不得分;



4. 绑定时间对象 匹配动作：记录 2 分，错配少配不得分;

22.DCBI 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期；（6 分）

1.ARP 统计：激活 3 分，错配少配不得分；

2.统计周期匹配题目要求参数 3 分，错配少配不得分；

23.DCBI 配置内网用户并发会话超过 1000，60 秒报警一次；（6 分）

1.并发会话：激活 3 分，错配少配不得分；

2.会话阀值、报警间隔匹配题目要求参数 3 分，错配少配不得分；

24.DCBI 配置监测到内网使用 RDP、Telnet 协议时，进行网页报警；（6 分）

1.添加黑名单协议匹配题目要求 3分，错配少配不得分；

2.动作：网页报警 3分，错配少配不得分；

25.DCBI 配置开启用户识别功能,对内网所有 MAC 地址进行身份识别；（6分）

勾选：按 MAC 识别 6分，错配少配不得分；

26.DCBI 配置统计出用户请求站点最多前 100 排名信息，发送到邮箱为 DCN2019@chinaskills.com；（6分）

1.报表 ： 用户请求站点最多排名 2分，错配少配不得分；

2.TOP:100 2分，错配少配不得分；

3.接收邮箱：2分，按试题中实际参数配置,错配少配不得分；

27.DCBI 配置创建一个检查 2019-05-01 至 2019-05-05 这个时间段邮箱内容包含“密码”的关键字的任务；（6分）

1.检索类别：邮件内容 2 分，错配少配不得分；

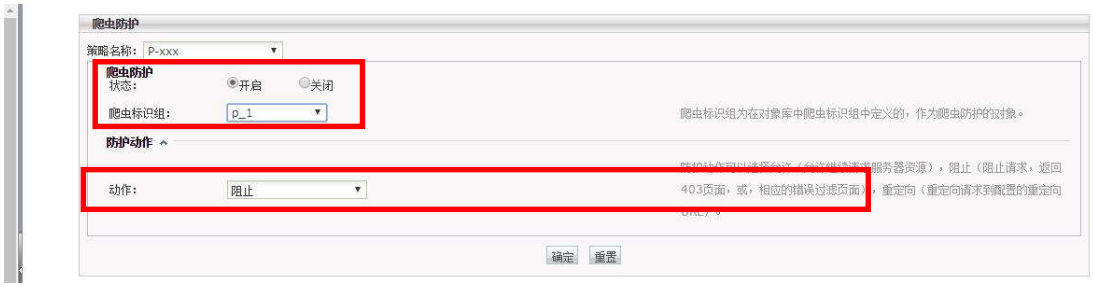
2.检索时间：2 分，错配少配不得分；

3.检索关键字匹配题目要求 2 分，错配少配不得分；

28.WAF 上配置开启爬虫防护功能，当爬虫标识为 360Spider，自动阻止该行为；（6 分）

1 分

1 分



1.创建爬虫标识爬虫标识组：2 分，错配少配不得分;

2.开启爬虫防护功能：2 分，错配少配不得分;

3 动作：阻止 2 分，错配少配不得分;

29.WAF 上配置开启防护策略，将请求报头 DATA 自动重写为 DATE;(6 分)

1.站点转换：开启 2 分，错配少配不得分;

2.站点转列表 ：动作、匹配值 、重写值符合题目要求 4 分，错配少配不得分;

30.WAF 上配置开启盗链防护功能，User-Agent 参数为 PPC Mac OS X 访问 www. DCN2019.com index.php 时不进行检查; （6 分）

1.开启盗链防护功能：2分，错配少配不得分；

2.允许进入页面/index.php,Referer URL www.DCN2019.com 2分，错配少配不得分；

3.例外检测域、例外检查值匹配题目要求：2分，错配少配不得分；

31.WAF上配置开启错误代码屏蔽功能，屏蔽404错误代码；(6分)

1.开启错误代码过滤功能：2分，错配少配不得分；

2.添加HTTP状态码匹配题目要求：4分，错配少配不得分；

32.WAF上配置阻止用户上传ZIP、DOC、JPG、RAR格式文件；（6分）

1.输入参数验证：开启 2 分，错配少配不得分；

2.动作：阻止 2 分，错配少配不得分；

3.上传文件格式 匹配题目要求：2 分，错配少配不得分；

33.WAF 上配置开启基本防护功能，阻止 SQL 注入、跨站脚本攻击；（6 分）

1.基本攻击防护：开启 2 分，错配少配不得分；

2.动作：阻止 2 分，错配少配不得分；

3.攻击防护类型，阻止 SQL 注入、跨站脚本攻击，2 分，错配少配不得分；

34.WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问*.bat 的文件;（6 分）

1.黑白名单：开启 2 分，错配少配不得分;

2.黑白名单种类、值，匹配题目参数 4 分，错配少配不得分;

35.无线控制器 DCWS 上配置管理 VLAN 为 VLAN101,第二个地址作为 AP 的管理地址,配置 AP 二层手工注册并启用序列号认证，要求连接 AP 的接口禁止使用 TRUNK; （6 分）

```
wireless
 no auto-ip-assign
 enable
 ap authentication serial-num
 static-ip  192.168.101.1
ap database 00-03-0f-8b-0c-30
  serial-num WL020420HC15002624
```

1.设置序列认证 2 分,错配少配不得分,序列号根据设备不同而不同。

```
Interface Ethernet1/0/3
  switchport mode hybrid
  switchport hybrid allowed vlan 10;20 tag
```

```
switchport hybrid allowed vlan 101 untag
switchport hybrid native vlan 101
```

2.E1/0/3 口下，native 101,允许 untag 101,tag 10,20 共 2 分，错配少配不得分;

3.设置给 AP 配置静态 ip 2 分，错配少配不得分;

36.无线控制器 DCWS 上配置 DHCP 服务，前十个地址为保留地址，无线用户 VLAN10,20，有线用户 VLAN 30,40 从 DCWS 上动态获取 IP 地址；（6 分）

```
service dhcp
!
ip dhcp excluded-address 172.16.10.1 172.16.10.10
ip dhcp excluded-address 172.16.20.1 172.16.20.10
ip dhcp excluded-address 172.16.30.1 172.16.30.10
ip dhcp excluded-address 172.16.40.1 172.16.40.10
```

1.设置排除地址 2 分，错配少配不得分。

```
ip dhcp pool vlan10
 network-address 172.16.10.0 255.255.255.0
```

```
 default-router 172.16.10.1
!
ip dhcp pool vlan20
 network-address 172.16.20.0 255.255.255.128
 default-router 172.16.20.1
!
ip dhcp pool vlan30
 network-address 172.16.30.0 255.255.255.192
 default-router 172.16.30.1
ip dhcp pool vlan40
 network-address 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
```

1 分

2.配置 4 个 DHCP 共 2 分，错配少配不得分;

DCRS:

```
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
  !forward protocol udp 67(active)!
 ip helper-address 192.168.100.254
!
interface Vlan20
 ip address 172.16.20.1 255.255.255.128
  !forward protocol udp 67(active)!
 ip helper-address 192.168.100.254
!
```

```
interface Vlan30
 ip address 172.16.30.1 255.255.255.192
  !forward protocol udp 67(active)!
 ip helper-address 192.168.100.254
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
  !forward protocol udp 67(active)!
 ip helper-address 192.168.100.254
!
```

3.4 个 ip helper-address 共 2 分，错配少配不得分;

37.在 NETWORK 1、2 下配置 SSID，需求如下:

1、设置 SSID DCN2019，VLAN10，加密模式为 wpa-personal,其口令为 DCN2019;

2、设置 SSID GUEST，VLAN20 不进行认证加密,做相应配置隐藏该 SSID; （6 分）

```
network 1
  igmp snooping m2u
  m2u threshold 8
  arp-suppression
  security mode wpa-personal
  ssid DCN2019
  vlan 10
```

3 分，错配少配不得分;

wpa key encrypted

e8e24f21e4796c6824984510dacb884070cb6df85eb6c7826c0ee8dd

f105225e20c61ed281962494fedee41218d3915b7684e01f159f0ae1

ba604fe0baf0161b（此处会被加密，不必一致）

time-limit from 00:00 to 06:00 weekday all

!

network 2

hide-ssid

ssid GUEST　3分，错配少配不得分;

vlan 20

!

network 3

38.配置SSID GUEST每天早上0点到6点禁止终端接入;（6分）

network 2

ssid GUEST

vlan 20

time-limit from 00:00 to 06:00 weekday all

!6分需在Network2下配置，否则不得分

39.在SSID DCN2019下启动组播转单播功能，当某一组播组的成员个数超过8个时组 播M2U功能就会关闭;（6分）

network 1

igmp snooping m2u　3分，错配少配不得分;

m2u threshold 8　3分，错配少配不得分;

arp-suppression

security mode wpa-personal

ssid DCN2019

vlan 10

需在 Network1 下配置，否则不得分。

40.开启 ARP 抑制功能，开启自动强制漫游功能、动态黑名单功能;（6 分）

dynamic-blacklist　2 分，错配少配不得分;

force-roaming mode auto　2 分，错配少配不得分;

network 1

igmp snooping m2u

m2u threshold 8

arp-suppression　2 分，错配少配不得分;